TREND MICRO™

ServerProtect⁵

Centrally managed virus protection for enterprise-class servers and storage systems

for NetApp

Getting Started Guide
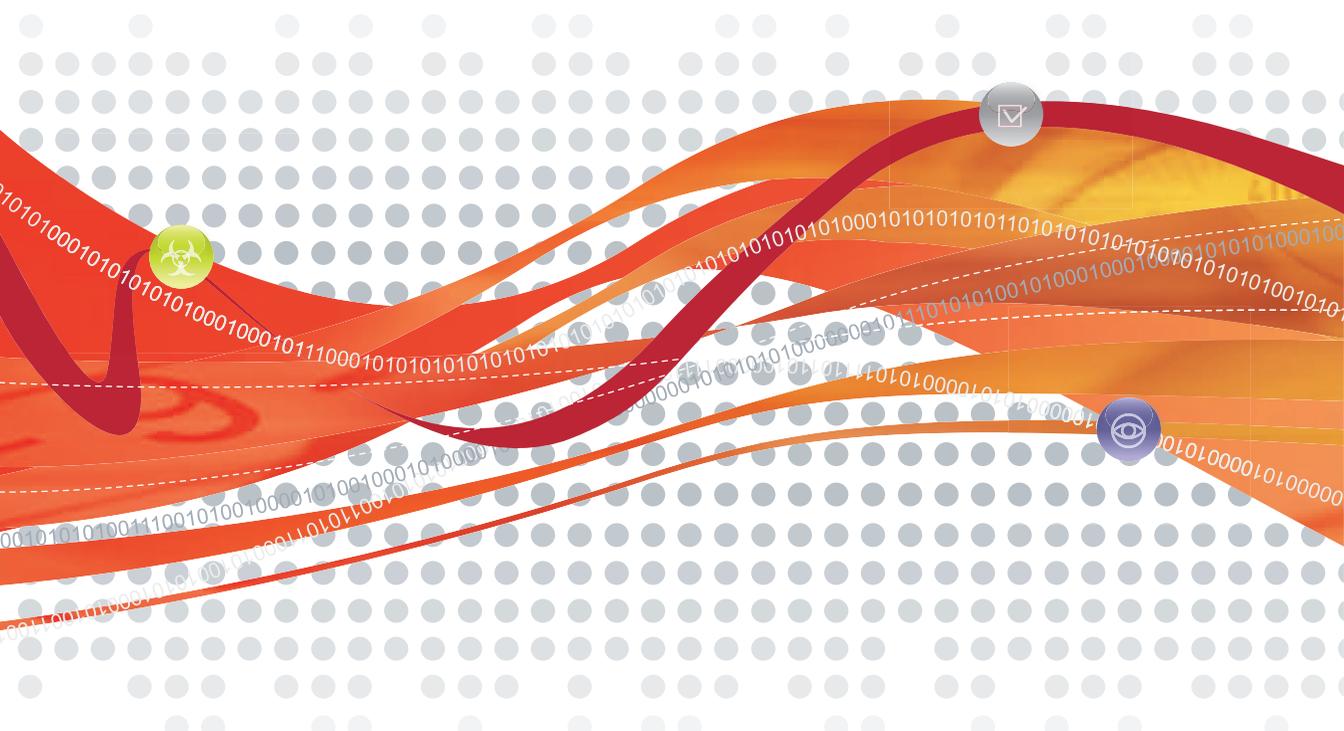
Award-Winning Antivirus Security

Anti-Spyware Defense

Endpoint Security

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

www.trendmicro.com/download/documentation/

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

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

www.trendmicro.com/license

Trend Micro, ServerProtect, Control Manager, MacroTrap, TrendLabs, and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated.

Microsoft Windows, Windows Server 2003, Windows Server 2008, Windows Storage Server 2003, Windows XP, Windows Vista, Windows 7, Windows NT, MS-DOS, PowerPoint, Excel, and Microsoft Office are trademarks of Microsoft Incorporated.

Intel®, and Pentium® are trademarks of Intel Corporation.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Document Part No. SPEM54352/91119

Release Date: March, 2011

Protected by U.S. Patent No. 5,951,698

The Getting Started Guide for Trend Micro™ ServerProtect™ 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 online knowledge base at the Trend Micro Web site.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at **docs@trendmicro.com**. Your feedback is always welcome. Please evaluate this documentation on the following site:
www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 1: Getting Started with Trend Micro™ ServerProtect™

Chapter 2: Installing ServerProtect for NetApp

Chapter 3: Managing ServerProtect

Chapter 4: Upgrade and Troubleshoot ServerProtect for NetApp

Chapter 5: Managing ServerProtect with Trend Micro Control Manager™

Chapter 6: Registering and Contacting Technical Support

Appendix A: Converting the ServerProtect Trial Version and FAQs

Index

Getting Started with Trend Micro™ ServerProtect™

ServerProtect is the latest generation of award-winning software for protecting file servers on corporate networks. It is designed specifically to protect the entire network from viruses of any kind by adopting advanced virus-catching technology to ensure that your network stays virus-free. ServerProtect detects new file infections, identifies viruses in existing files, and detects activity indicating an "unknown" virus may have entered the network environment on either the server or workstation.

ServerProtect enables network administrators to manage multiple Microsoft Windows network servers from a single portable management console. The console enables administrators to simultaneously configure servers in the same domain and generate integrated virus incident reports from each one.

By giving administrators a means to configure, monitor, and maintain antivirus efforts through the ServerProtect Management Console, ServerProtect improves and simplifies the implementation of corporate virus policy. This results in lower virus protection costs.

Trend Micro ServerProtect for NetApp is an enhanced version of ServerProtect developed exclusively to provide antivirus solutions for NetApp Filers. Scalable and reliable, ServerProtect for NetApp protects NetApp's line of Filer storage appliances against viruses, Trojans, and other malicious codes.

The topics included in this chapter are:

What's New in SeverProtect for NetApp Version 5.8

- Support for Microsoft Windows Server platforms including most versions in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 servers (See *System Requirements* on page 2-2)

- VMWare ESX/ESXi version 3.5/4.0/4.1 server support

- New spyware pattern support to detect virus infections, which also includes new features to perform quarantine, delete, and renaming actions for handling infected files

- Upgrade from ServerProtect 5.62 by running either the installation program or deployment program

- Enhanced security when communicating between the Information Server and Windows Normal Server

- Latest Damage Cleanup Engine and Anti-Rootkit module as a generic cleaning feature

- Supports BlueArc Mercury Network Storage System

- Support Trend Micro Control Manager 5.5

How Does ServerProtect Work?

ServerProtect monitors all activity in a file server network. Whenever ServerProtect detects that a file in its domain is being accessed, it checks the file for infection.

If it finds that the file is infected, it sends notification messages to pre-defined recipients and takes action on the virus according to the ServerProtect configuration. The ServerProtect activity log records all the activities of the system.

ServerProtect allows you to design personal scanning profiles—saving you from having to re-configure frequently needed settings. You can even assign multiple scanning options to a profile and use the profile for special circumstances, for example: scanning incoming files only.

How Does ServerProtect Manage Servers?

ServerProtect secures your client/server network using a three-tier architecture: the Management Console, the Information Server (middleware), and the Normal Server. Together, these components create a powerful, centrally managed, cost-effective antivirus security system.

The Management Console provides a user-friendly, Windows-based interface for configuring system components. Management Console instructions are sent to the Information Server, which then passes them on to the Normal Servers.

ServerProtect for NetApp scans viruses using "on-access" mode, which takes place on a Scan Server. In turn, the Information Server manages the Scan Servers.

Communication Methods

The Management Console uses Transmission Control Protocol/Internet Protocol (TCP/IP) with a password-protected logon to communicate with the Information Server. The Information Server uses a Remote Procedure Call (RPC) to connect to Windows.

ServerProtect Architecture

ServerProtect protects networks through a three-tier architecture: the Management Console, the Information Server, and the Normal Server. The following illustrates the relationship between these three components:
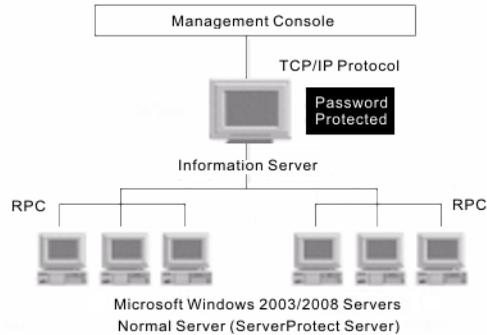
FIGURE 1-1.   ServerProtect three-tier architecture

The Management Console

The ServerProtect Management Console is a portable console which gives network administrators centralized control of multiple network servers and domains. The console enables you to simultaneously configure Normal Servers in a specified domain and generate integrated virus incident reports for them. The Management Console contains the following items:

- Main menu
- Side bar (Shortcut bar)
- ServerProtect domain browser tree
- Configuration area

The ServerProtect domain browser tree shows all the ServerProtect Normal Servers in the domain, the status information of each server including the version of the virus pattern, the version of the scan engine file, type and that of the operating system, data flow direction of real-time scanning and others. Note that the administrator can configure how all this data is displayed.

Tip: You can use the Management Console to remotely install one or more Normal Servers. See *Installing a Normal Server* on page 2-19.

The Information Server

An Information Server is the main communication hub (middleware) between the Management Console and the Normal Servers it manages. It simplifies control of Normal Servers by allowing administrators to send instructions and receive information from remote sites.

WARNING!   **An Information Server by itself is defenseless unless a Normal Server is installed on the same computer.**

Information Server Tips

- If you are performing the very first ServerProtect installation on your network, you need to set the destination server as an Information Server, and then configure the other Normal Servers to this Information Server.

- An Information Server must have at least one member domain for supporting Normal Servers.

- Because an Information Server is simply a delivery system for information, the number of Normal Servers it can manage is, theoretically, only limited by the available bandwidth. You might, however, choose to moderate the number of Normal Servers you assign to an Information Server for ease of management.

- If you have many servers in different locations, set up an Information Server (IS) in each location.

> **Note:** Benchmark testing results have verified that an Information Server can manage up to 250 Normal Servers. This number serves as a reference only. The Information Server can manage more Normal Servers depending on the available bandwidth.

> **Note:** The Information Server and the Management Console are native 32-bit components of ServerProtect. However, on the 64-bit platform, these components of ServerProtect will run on **Windows On Windows (WOW)** 64 mode.

The Normal Server

A Normal Server can be any server on a network where ServerProtect is installed. This is the first line of defense in the ServerProtect architecture and where all the action takes place. These servers perform the actual antivirus functions of the system, and are managed by an Information Server.

> **Note:** If the Normal Server is used to protect NetApp Filers, then it can also be referred as "Scan Server".

ServerProtect offers several ways for installing Normal Servers:

- Using the setup program. See *Installing a Normal Server from the Setup Program* on page 2-20.
- Using the Management Console. See *Installing a Normal Server from the Management Console* on page 2-23.
- Using Microsoft Server Management Server (SMS). See *Deploying through Microsoft SMS* on page 2-24.
- Using silent mode. See *Installing ServerProtect in Silent Mode* on page 2-32.

Each of the listed installation methods can be tailored to your specific company needs. See *Installing a Normal Server* on page 2-19.

Note: If the operating system is 32-bit, then 32-bit binaries of the Normal Server component of ServerProtect will be installed. If the operating system is 64-bit, then 64-bit binaries of Normal Server component of ServerProtect will be installed.

WARNING!   **Because it is time-consuming to install servers individually from the setup program, Trend Micro recommends that you install your servers from the ServerProtect Management Console.**

ServerProtect Domains

ServerProtect domains are virtual groupings of Normal Servers used to simplify their identification and management. You can create, rename, or delete domains according to the needs of your network.

Normal Servers in a domain can only be assigned to one Information Server. Information Servers, on the other hand, can manage several domains.

The most efficient way to manage network protection is to group all servers in relevant ServerProtect domains. For example, you can create a ServerProtect domain called "NS" to manage Normal Servers more efficiently. See *Managing ServerProtect Domains* on page 3-9.

WARNING!   **The concept of ServerProtect domains are not that of a Microsoft Windows domain; it is simply a logical grouping of Normal Servers running ServerProtect.**

ServerProtect domains have the following features:

•   **Domain filter**: Network administrators can set up a filter on an Information Server to control what can be viewed from the domain browser tree on the Management Console.

•   **Flexible domain management**: After logging on to the console, IT professionals can add, rename, or delete domains according to their preference.

Note: The main feature of the Management Console is to centralize the control multiple Normal Servers via a number of Information Server. However a Management console can only connect to and control one Information Server at any given time.

ServerProtect for NetApp Architecture Overview

ServerProtect for NetApp scans viruses using "on-access" mode, which takes place on a Scan Server. In turn, the Information Server manages the Scan Servers.
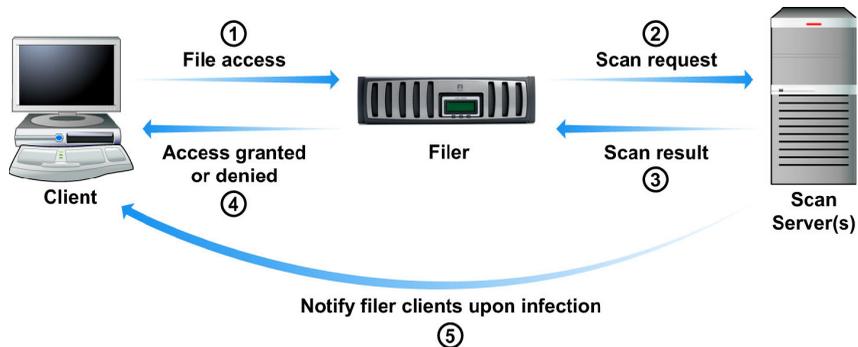
FIGURE 1-2.   ServerProtect for NetApp Product Architecture

When a ServerProtect for NetApp user tries to access a file or store a new file in a NetApp Filer, the NetApp Filer performs a virus check. If the filename extension matches the file scanning criteria (for example, an ".EXE" or a ".VBS" file), the NetApp Filer sends a manual scan request (Scan Now) to the Scan Server(s). The Scan Server then passes back the scan result to the NetApp Filer and according to the scan result, the user is either allowed to open, save, or is denied access to the file. To learn more about setting your NetApp Filer file scanning criteria, refer to your NetApp Filer documentation.

Note:	Since only specific file types contain viruses, establishing the right file scanning criteria can help optimize Scan Server performance, reduce bandwidth usage, and minimize scanning time. To learn how ServerProtect for NetApp can efficiently and safely scan files, see *IntelliScan* on page 1-20.

If a file contains a virus, ServerProtect for NetApp performs a designated action. Refer to See *Scanning Viruses* on page 3-54 for additional information about scan actions. For example, if the file is cleanable and ServerProtect for NetApp is configured to perform a Clean action, the following will occur:

1. The Scan Server cleans the file and informs the NetApp Filer that the file is no longer infected.

2. The NetApp Filer allows its client to access the cleaned file and replaces the original file with the cleaned one.

Note:	The NetApp Filer "trusts" registered Scan Servers. Therefore, if a Scan Server also functions as a Normal Server (as a file or data server) and happens to send a file to the NetApp Filer, it will not request the file to be scanned. To protect both the NetApp Filer, and the Normal Server, set the ServerProtect Real-time Scan to "Incoming & outgoing". See See *Configuring Scan* on page 3-58 to set Real-time Scan to Incoming & outgoing.

Organizational Overview

Below is an explanation of the ServerProtect for NetApp organizational flow:
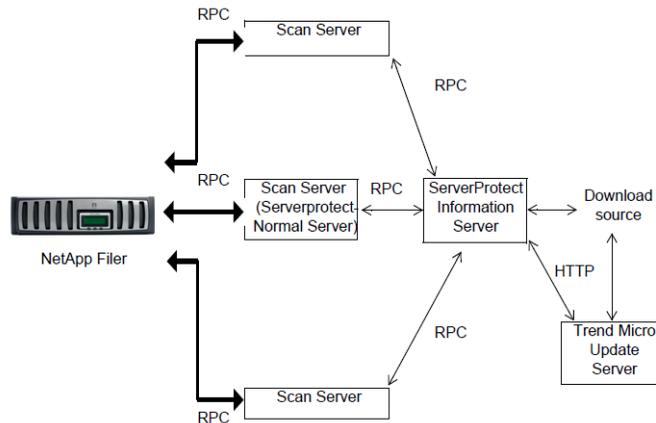
FIGURE 1-3.   ServerProtect for NetApp organizational flow

ServerProtect for NetApp consists of an agent that communicates with the NetApp Filer via remote procedure calls (RPCs). This agent performs the following functions:

- Registers the Normal Server with the NetApp Filer as a "Scan Server." This informs the NetApp Filer of the availability and location of a Scan Server
- Watches for NetApp Filer file-scanning requests
- Returns scan results to the NetApp Filer
- Answers any queries from the NetApp Filer
- Informs the NetApp Filer of any pattern file or scan engine updates

Communicates with the NetApp Filer to check the connection between the Scan Server and the NetApp Filer

Real-time Scan Versus On-demand Scan (Scan Now)

ServerProtect features two powerful scan functions, Real-time Scan and Scan Now.

Real-time Scan runs continuously on a server and provides the maximum level of virus protection. All file I/O events on the server are monitored and infected files are prevented from being copied to or from the server. See *Using Real-Time Scan* on page 3-58.

Scan Now is a manual virus scan (that is, it occurs immediately after being invoked). Use Scan Now to check a server that you suspect may have been exposed to a computer virus or about which you want immediate information. See *Using Scan Now (Manual Scan)* on page 3-61.

Tip: To ensure maximum protection, Trend Micro recommends using both Real-time Scan and Scan Now.

Real-time Scan and Scan Now benefits include:

- **Redundant File Scan**: If a file containing a virus is accidentally downloaded or copied, Real-time Scan will stop it. Even if for any reason Real-time Scan is disabled, Scan Now will still detect it.

- **Efficient File Scan**: By default, Real-time Scan is configured to scan files. It has the advantage of minimizing the impact to system resources. See *Scanning Viruses* on page 3-54.

- **Effective and Flexible File Scan**: ServerProtect gives IT professionals effective and numerous scan configuration options to protect their networks based on their individual needs. See *Scanning Viruses* on page 3-54.

Working with Tasks

ServerProtect allows IT professionals to create multiple tasks which can be deployed on demand or on a scheduled basis.

Use ServerProtect tasks to:

- Deploy updates
- Run Real-time Scan
- Run Scan Now
- Purge, export, or print logs
- Generate virus scan statistics

ServerProtect tasks benefits include:

- Simultaneous multiple function deployment
- Unattended routine antivirus maintenance procedures on your network
- Improved antivirus management efficiency and control over antivirus policy

Tasks are assigned to a "task owner" who is responsible for maintaining the task. See *Managing Tasks* on page 3-36.

After you install ServerProtect on a server, three default tasks already exist: Scan, Statistics, and Deploy. These tasks are essential for managing and monitoring antivirus activities on your network. You can modify the target servers of these three default tasks, as well as their definitions.

When ServerProtect Finds a Virus (Virus Actions)

ServerProtect allows you to configure the type of action that the software takes on infected files. In addition to the antivirus protection offered by previous versions, a Spyware pattern is now available in ServerProtect 5.8, forming a virus category of its own. You can choose a specific course of actions to handle certain types of viruses at will. The Damage Cleanup Engine is made more powerful by including the feature of Generic Clean.

There are five possible actions that ServerProtect can take on an infected file:

- **Bypass (Ignore)**: For a manual scan, ServerProtect skips the file without taking any corrective action. However, detection of the virus is still recorded in the program's log entries. For Real-time Scan, ServerProtect treats the file as "deny-write," protecting it from duplication or modification. See *Defining Actions Against Viruses* on page 3-55 for more information.

- **Delete**: The infected file is deleted.

- **Rename**: The infected file extension is renamed to .vir. This prevents the file from being executed or opened. If a file of that name with the .vir extension already exists, the file will be renamed to .v01, .v02, and so on, until .v99.

- **Quarantine**: The infected file is moved to a folder of your choice. You can also change the file extension of the moved file to prevent it from being inadvertently opened or executed.

- **Clean**: Attempt to clean the virus code from the file. Because the cleaning process sometimes corrupts the file and makes it unusable, you can back up the file before cleaning.

All virus events and associated courses of action are recorded in the log file. For more information, refer to the *Viewing the infection logs* topic in the online help and *Defining Actions Against Viruses* on page 3-55.

Note: If you select **Clean** as the virus action, you can specify a secondary action if the cleaning process is unsuccessful.

Note: On a 64-bit operating system, ServerProtect detects both 32-bit viruses and 64-bit viruses.

Note: ServerProtect 5.8 does not support clean action against spyware infected files. When using ActiveAction, the actual effect of an action applied to a spyware infected file will be equivalent to that of the Bypass action.

Note: By default, NetApp Filers do not include ".ZIP" in the set of file extensions to be scanned. To enable scanning for ".ZIP" and other file types, see *Selecting File Types to Scan* on page 3-66. This also applies to other types of compressed files.

Virus Logs

The real power of a centralized antivirus system is its ability to record and present information regarding the network's antivirus policy from a single console. IT professionals can easily access information while they are monitoring their network servers.

ServerProtect provides comprehensive information about scanning, file updating, and deploying results. Furthermore, ServerProtect saves the information in a log file which can be either retrieved or exported. For example, you can analyze the scanning statistics for virus scanning on your network. These statistics include information such as what the most common viruses are or which users introduced viruses to the network. In addition, you can export the log information to a database or spreadsheet application for further analysis.

On each Normal Server, ServerProtect 5.8 supports backing up of log database file when it exceeds the default size limit of 10-MB or after configured number of days. The default size for the log file is 8000 entries, or up to 10-MB. After the log file exceeds 8000 entries or 10-MB, which ever is smaller in size. ServerProtect automatically renames the log file and creates a new log file. ServerProtect, however, does not impose number of days limit, unless it is configured. For information on configuring log backup, refer to *Configuring the Log Database Backup Options* topic in Online Help.

You can also take action on the infected files directly from the Scan Result window, providing you a convenient way to take appropriate actions on a virus infection event. For more information about log files, refer to the ServerProtect online help from the ServerProtect Management Console. For more information on Virus logs, refer to the *Viewing log information* and *Viewing Information Server logs* topics in the Online Help.

Deploying Updates

Trend Micro update is an upgrade and update deployment module for Trend Micro antivirus software. It simplifies the maintenance of Trend Micro software and reduces the total cost of your network's antivirus security. Because of the number of viruses that are developed monthly, a successful virus policy depends on the use of virus pattern files and scan engine files, that can deal with the latest threats. See *Configuring Updates* on page 3-23.

Note: Trend Micro releases new versions of these downloadable update files on a regular basis.

ServerProtect update features include:

- **Update component selection:** Trend Micro provides a rich set of anti virus utilities in ServerProtect 5.8 for updating, including newly-added Spyware pattern and other virus patterns, Damage Cleanup Engine and a Damage Cleanup Template, as well as Anti-rootkit driver.

- **Unattended scheduled update**: You can create scheduled update tasks to update all Normal Servers while you are asleep.

- **Flexible file download**: You can designate an Information Server to download updates from the Trend Micro update site, then have other servers obtain the updated files from it.

- **Centralized update deployment:** You can deploy updates to servers on your network from the Management Console.

- **Firewall and proxy server compatibility**: ServerProtect works with the majority of existing firewalls and proxy servers.

- **Update activity logging**: ServerProtect records all update activity in a log file for future reference.

- **Update Roll-back option**: If you encounter a problem while deploying an update, you can only roll-back the component which is most recently updated. Note that the rollback operation can only be carried out on virus patterns and Virus Scan Engine.

Note: The version 5.8 ServerProtect now supports the update of program files.

Updating ServerProtect is a two-step process:

1. Download updates from the Trend Micro update server. See *Downloading Updates* on page 3-26.

2. Deploy the downloaded updates to other Normal Servers on the network. See *Deploying Updates* on page 3-31.

This highly efficient approach saves download time and minimizes network bandwidth usage.

Tip: You can automate the deployment of updates for Normal Servers by creating a scheduled update task. See *Creating Tasks* on page 3-38.

ServerProtect Virus Detection Technology

ServerProtect uses advanced virus detection technology. In this section, we feature the tools which support this state of the art technology and how IT professionals can benefit from it.

Pattern Matching

Using a process called "pattern matching," ServerProtect draws on an extensive database of virus patterns to identify known virus signatures. Key areas of suspect files are examined for tell-tale strings of virus code and compared against thousands of virus signatures that Trend Micro has on record.

For polymorphic or mutation viruses, the ServerProtect scan engine permits suspicious files to execute in a protected area within which it is decrypted. ServerProtect then scans the entire file, including the freshly decrypted code, and looks for strings of mutation-virus code.

If such a virus is found, ServerProtect performs the action you previously specified to handle it. ServerProtect virus actions include **clean** (autoclean), **delete**, **bypass** (ignore), **quarantine** (move), or **rename**. Virus actions can be customized for both boot viruses and file viruses. See *Scanning Viruses* on page 3-54.

> **Note:** It is important to keep the Spyware pattern and virus pattern files up to date. More than a thousand new viruses are created each year. Trend Micro makes it easy to update the pattern file by supporting scheduled updates. See *Configuring a Scheduled Deployment* on page 3-33 and *Configuring a Scheduled Deployment* on page 3-33 for more information.

MacroTrap™

ServerProtect includes patented MacroTrap™ technology to guard against macro viruses in Microsoft™ Office files and templates. Macro viruses are the fastest spreading computer viruses. Because they are harbored in files that are commonly passed around by email, these kinds of viruses are easily spread. See *Configuring Scan* on page 3-58 for MacroTrap configuration information.

> **Note:** Trend Micro MacroTrap protects network users from receiving and sending macro viruses.

How MacroTrap Works

The MacroTrap performs a rule-based examination of all Macro code that is saved in association with a document. Macro virus code is typically contained as a part of the invisible template (for example, `*.dot` in Microsoft Word) that travels with the document. Trend Micro MacroTrap checks the document for signs of a macro virus by seeking out instructions that perform virus-like activity. Examples of virus-like activity are copying parts of the template to other templates (replication), or code to execute harmful commands (destruction).

Compressed Files

Compressed file archives (that is, a single file composed of many separate compressed files) are the preferred form to distribute files by email and the Internet. Because some antivirus software is not able to scan these kinds of files, compressed file archives are sometimes used as a way to "smuggle" a virus into a protected network or computer.

The Trend Micro scan engine can scan files inside compressed archives. It can even scan compressed files that are composed of other compressed files -- up to a maximum of five compression layers.

The Trend Micro scan engine used in ServerProtect can detect viruses in files compressed using the following algorithms:

- PKZIP (.zip) and PKZIP_SFX (.exe)
- LHA (.lzh) and LHA_SFX (.exe)
- ARJ (.arj) and ARJ_SFX (.exe)
- CABINET (.cab)
- TAR
- GNU ZIP (.gz)
- RAR (.rar)
- PKLITE (.exe or .com)
- LZEXE (.exe)
- DIET (.com)
- UNIX PACKED (.z)
- UNIX COMPACKED (.z)
- UNIX LZW (.Z)
- UUENCODE
- BINHEX
- BASE64

Note: The Trend Micro scan engine can currently only clean compressed files using the PKZIP algorithm. If a virus is found in an archive using other algorithms, they must first be decompressed in a temporary directory, then cleaned.

For compressed file configuration information, refer to *Configuring Scan* on page 3-58, and *Configuring Scan Now* on page 3-61.

Damage Cleanup Services

Damage Cleanup Services (DCS) detects Trojans, based on their behavior, and restores modified system files. DCS also terminates Trojan-related processes, and deletes files that the Trojan "drops" in the system.

Note: If a spyware infected file is detected, only bypass can be applied. The file will be bypassed without any other treatment. Clean function does not apply to spyware infection.

OLE Layer Scan

Microsoft™ Object Linking and Embedding (OLE) allows embedding Microsoft Office™ files within themselves. This means that you could have a Microsoft Word document inside an Excel spread sheet, and in turn this Excel spread sheet could be embedded in a Microsoft™ PowerPoint presentation.

OLE offers a large number of benefits to developers, at the same time it can lead to potential infection. To address this issue, Trend Micro has added a new scan feature "OLE layer scan" that complements state-of-the-art ServerProtect virus protection. See *Scanning Viruses* on page 3-54.

Tip: OLE layer scan offers five layers of protection. Trend Micro recommends a setting of two OLE layers for Scan Now and a setting of one for a Real-time Scan. A lower setting will improve server performance.

IntelliScan

IntelliScan is a new method of identifying which files to scan that is both more secure, and more efficient, than the standard "Scan All files" option.

For executable files (that is, `.zip`, `.exe`), the true file type is determined from the file content. In the event that a file is not executable (such as `.txt`), IntelliScan will use the file header to verify the true file type. See *Scanning Viruses* on page 3-54.

The following are just a couple of the benefits IntelliScan offers to administrators:

- **Performance optimization**: Server system resources allotted to scan will be minimal, thus using IntelliScan will not interfere with other crucial applications running on the server.

- **Time saving**: Because IntelliScan uses true file type identification, IntelliScan scan time is significantly less than that of all files scan (this means that only files with a greater risk of being infected are scanned). This time difference is noticeable when you use IntelliScan with Scan Now. See *Configuring Scan Now* on page 3-61.

ActiveAction

ActiveAction is a set of pre-configured scan actions that can be performed on viruses and other types of malware. ActiveAction can be configured for both Scan Now and Real-time Scan.

When to Select ActiveAction

Trend Micro recommends that you select ActiveAction if you are not familiar with virus actions or if you are unsure of which scan action is the most suitable for a certain virus.

Viruses vary significantly from one another; this requires appropriate virus actions for each virus type. Customizing scan actions for file viruses requires knowledge of viruses and can be a tedious task. For this reason, Trend Micro recommends the use of ActiveAction.

Some advantages of using ActiveAction versus customized scan actions are:

- **Time saving**: You spend no time customizing virus actions.

- **Worry-free maintenance**: ActiveAction uses Trend Micro recommended scan actions so you can concentrate on other tasks and not worry about making mistakes.

- **Updateable scan actions**: Trend Micro includes new ActiveAction scan actions with every new pattern. Viruses constantly change how they attack, thus scan actions should be frequently modified to prevent possible infection.

For ActiveAction configuration information, See *Defining Actions Against Viruses* on page 3-55.

Note: When using ActiveAction, the action for spyware virus is bypass/bypass.

Mapped Network Drive Scan

ServerProtect can scan one or several network drive(s); the shared network folders have to be mapped first before selecting this feature. This is helpful because Real-time Scan scans and protects mapped drives as it does with local drives, therefore reducing the risk of infection. See *Configuring Scan* on page 3-58

Additional Features

To help IT professionals protect their networks with more flexibility, ServerProtect includes additional features.

Centralized Management

ServerProtect provides a Windows-based console (the Management Console) to help you manage virus protection for multiple servers on your network. The console is portable and can be run on any 32-bit or 64-bit Windows Server.

Enhanced Network Security on Installation

During Normal or Information Server installation, you must enter the administrator user name and password of the selected target servers.

Swift Response to Virus Outbreaks

If a virus tries to infect a file in a shared folder on a server under the protection of ServerProtect, a message box appears, identifying the computer in the network on which the virus originated from. This message box also displays the following information: the type of scan, the name of the virus, the name of the infected file, the name or ID of the computer involved and the user name. In addition, it also displays the action taken on the virus and the source of infection. See *Configuring Notification Messages* on page 3-47.

Flexible Control over Infected Files

When ServerProtect detects an infected file, you can choose to restore the file after cleaning, send suspect or uncleanable files to Trend Micro, delete the backup file made before cleaning, or return cleaned files to the user by email.

NetworkTrap Tool

Certain viruses actively seek out shared folders (an example of this type of virus is PE.FunLove.4099) to infect as many connected users as possible. The NetworkTrap tool lets you share a folder and automatically copies the contents of the Bait folder to the newly created shared folder (the Bait' folder contains files that viruses are likely to infect). This shared folder works with the new virus notification to create an effective virus trap. For more information on this topic, refer to the *NetworkTrap Tool* section in the online help.

State-of-the-Art Virus Detection Technology

New configurable scanning tools like ActiveAction, IntelliScan, and OLE layer scan offer faster and more efficient scanning.

Viewable Scanning Statistics

ServerProtect enables you to efficiently monitor your network antivirus security. It displays scanning statistics on your network, including the following, for a given interval: total number of viruses found, top ten viruses found, top ten infected users, total number of non-cleanable viruses, and more.

Compatibility

ServerProtect is fully compatible with Microsoft Windows Server 2003 and 2008 operating systems. It also supports Network File System (NFS) drivers, and SOCKS 4 for the Trend Micro update server.

ServerProtect is compatible with 32-bit and 64-bit operating systems. ServerProtect automatically detects 32-bit and 64-bit Windows Servers. If the operating system is 32-bit, then 32-bit binaries of the Normal Server component of ServerProtect will be installed or uninstalled. If the operating system is 64-bit, then 64-bit binaries of the Normal Server component of ServerProtect will be installed or uninstalled.

Installing ServerProtect for NetApp

This chapter includes the following information to successfully install ServerProtect for NetApp on your network(s):

Note: You must log on with administrator privileges in order to install an Information Server.

Note: You cannot install a previous version of Normal Server and register it to the ServerProtect 5.8 Information Server.

System Requirements

Normal Server

- CPU: 2.5-GHz Intel™ Pentium™ IV processor or 3.0-GHz EM64T Intel™ processor or 2.0-GHz AMD Athlon™ 64-bit processor (or equivalent)
- DRAM: Minimum 1-GB, 2-GB recommended
- Operating System:
    - Microsoft Windows Server 2003 Standard or Enterprise SP2 or above (x86)
    - Microsoft Windows Server 2003 Standard or Enterprise SP2 or above (x64)
    - Microsoft Windows Server 2003 R2 Standard or Enterprise SP2 (x86)
    - Microsoft Windows Server 2003 R2 Standard or Enterprise SP2 (x64)
    - Microsoft Windows Server 2008 Standard or Enterprise SP2 (x86)
    - Microsoft Windows Server 2008 Standard or Enterprise SP2 (x64)
    - Microsoft Windows Server 2008 R2 Standard or Enterprise SP1 (x64)
    - Microsoft Windows 2008 Server Core
- Disk Space: 1-GB.
- 120-MB disk space is required, extra 20-MB if installation of Trend Micro Control Manager Agent is needed.
- A CD-ROM drive if the installation is performed locally.
- Network protocols and services: TCP/IP, Microsoft Network and RPC services must be running on Windows Server family operating system.

Information Server

- 3.0-GHz Intel™ Pentium™ IV processor or 3.0-GHz EM64T Intel™ processor or 2.0-GHz AMD Athlon™ 64-bit processor (or equivalent)
- DRAM: Minimum 1-GB, 2-GB recommended
- Operating System:
    - Microsoft Windows Server 2003 Standard/Enterprise SP2 or above (x86)
    - Microsoft Windows Server 2003 Standard/Enterprise SP2 or above (x64)
    - Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 (x86)

- • Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 (x64)
    - • Microsoft Windows Server 2008 Standard/Enterprise SP2 (x86)
    - • Microsoft Windows Server 2008 Standard/Enterprise SP2 (x64)
    - • Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 (x64)
- • Disk Space: 1-GB
- • A CD-ROM drive if the installation is performed locally.
- • Network protocols and services: TCP/IP, Microsoft Network and RPC services must be running on Windows Server family operating system.

The services listed above must be running on the installed machine. Trend Micro recommends an allocated bandwidth usage of minimum 128 Kilobytes per second to optimize deployment of component updates between ServerProtect Information Server and Normal Server. If RPC communication is non-functional, ServerProtect 5.8 will automatically switch to another protocol, either named pipe or TCP. To manage Windows Server, an Information Server must be installed.

Note: For ActiveUpdate 2.8, additional 500-MB disk space is required if Smart Duplicate is needed to be turned on, in which case the cashed pattern number must be set to value of 147.

Management Console

- • 2.5-GHz Intel™ Pentium™ IV processor or 3.0-GHz EM64T Intel™ processor or 2.0-GHz AMD Athlon™ 64-bit processor (or equivalent)

For Server Environment:

- • DRAM: Minimum 1-GB, 2-GB recommended
- • Operating System:
    - • Microsoft Windows Server 2003 Standard/Enterprise SP2 or above (x86)
    - • Microsoft Windows Server 2003 Standard/Enterprise SP2 or above (x64)
    - • Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 (x86)
    - • Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 (x64)
    - • Microsoft Windows Server 2008 Standard/Enterprise SP2 (x86)
    - • Microsoft Windows Server 2008 Standard/Enterprise SP2 (x64)

- Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 (x64)

For Client Environment:

- DRAM: Minimum 512-MB, 1-GB recommended
- Operating System:
    - Microsoft Windows XP Professional SP2 or SP3 (x86)
    - Microsoft Windows XP Professional SP1 or above (x64)
    - Microsoft Windows Vista Business/Enterprise/Ultimate SP1 (x86)
    - Microsoft Windows Vista Business/Enterprise/Ultimate SP1 (x64)
    - Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 (x86)
    - Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 (x64)
- Disk Space: 500-MB

VMWare

- VMWare ESX/ESXi 3.5/4.0/4.1
- VMWare Workstation 5.0 or above

Hyper-Visor

- Microsoft Windows Server 2008 R2 Standard/Enterprise with Hyper-V
- Microsoft Windows Server 2008 Standard/Enterprise with Hyper-V

NetApp Filer and BlueArc Network Storage

To communicate with ServerProtect, virus scan function must be enabled on NetApp Filer and BlueArc Network Storage.

The NetApp Filer proprietary OS:

- Data ONTAP™ 7.x Series
- Data ONTAP™ 8.0 7-Mode

BlueArc Mercury Network Storage System:

- System Management Unit (SMU) 7.0.2050

For optimal scanning performance, Trend Micro recommends the connection between NetApp filer or BlueArc NAS and a Scan Server to have a bandwidth of at least 1-gigabit per second.

Note: Scan Server must be located in the same domain as the BlueArc Storage System to correctly support the virus scan option.

Installation Scenarios

This section will help you select the most appropriate scenario to install ServerProtect on your network(s). The following scenarios focus on Local Area Networks (LANs), although it is also possible to manage ServerProtect across Wide Area Networks (WANs) such as, corporate Intranets, using TCP/IP. See *Managing ServerProtect Across a Wide Area Network* on page 2-9.

Specifying Your Installation Environment

Trend Micro ServerProtect supports Microsoft Windows platform. If you are installing ServerProtect on your network for the first time, you must set the destination server as an Information Server, then configure the Normal Servers to join it. An Information Server must have at least one ServerProtect domain to manage its Normal Servers. See *ServerProtect Domains* on page 1-8.

Note: If you have many servers concentrated in different geographical locations, set up an Information Server (IS) in each location. See *Information Server Tips* on page 1-6.

The following table shows the different installation environments for each ServerProtect setup component on Microsoft Windows platforms

TABLE 2-1.   **Installation Scenarios on MS Windows**

Operating System	Information Server	Normal Server	Management Console
Windows Server 2003 family 32-bit	Yes	Yes	Yes
Windows Server 2003 family 64-bit	Yes (WOW64)	Yes	Yes (WOW64)
Windows Server 2008 family 32-bit	Yes	Yes	Yes
Windows Server 2008 family 64-bit	Yes (WOW64)	Yes	Yes (WOW64)
Windows 2008 Server Core 32-bits	No	Yes	No
Windows 2008 Server Core 64-bits	No	Yes	No
Windows XP Professional	No	No	Yes
Windows Vista desktop family	No	No	Yes
Windows 7 desktop family	No	No	Yes

Note: **Windows** Server **2003** family means Standard version, Enterprise version, Storage server.

    Windows Server **2008** family means Standard version, Enterprise version, Storage server.

    Windows Vista desktop family means Business version, Enterprise version and Ultimate version.

    Windows 7 desktop family means Professional version, Enterprise version and Ultimate version.

Note: Hyper-V is supported by Windows Server 2008 64-bit.

Firewall Setting for ServerProtect Components

This page describes the setting of firewall. Please make sure configure your firewall correctly to make the communication open.

Firewall Setting for Machine with Management Console

• Open 1000-1009 port for TCP protocol

1000-1009 is used by Management console to receive the event back message from information server.

Management console will listen at the port 1000 when startup. If the port is occupied by other program, management console will find one available port from 1000 - 1009.

Firewall setting for Information Server

• Open 5005 - 5014 ports in TCP protocol.

Port 5005 is used to receive the commands from Management Console. Normally, 5005 must be opened. If it is used by other program, please find one available port from 5006-5014 and open firewall setting.

• Open 3000 - 3009 (UDP)

Port 3000 is used to receive broadcast message. If port 3000 is occupied by certain program, please find one available port from 3000 - 3009 one by one and open the firewall.

• Open 137 - 139 for RPC Over named pipe.

   ◆ 137 (UDP)

   ◆ 138 (UDP)

   ◆ 139 (TCP)

Note: These ports are opened to enable ServerProtect to use Remote Procedure Call (RPC) to communicate.

• Open 3628(TCP)

Port 3628 is used to receive event back.

• Open 1921 for SPX/TCP with Netware

Port 1921 is used to communicate with Netware in SPX/TCP protocol.

Firewall Setting for Windows with Normal Server

• Open 5168 for listening RPC over TCP/IP from Information Server

Port 5168 is used to receive commands from information server.

• Open 137 - 139 for named pipe.
  ◆ 137 Protocol is UDP.
  ◆ 138 Protocol is UDP.
  ◆ 139 Protocol is TCP.

Firewall setting in the netware machine with normal server.

• Open port 9921 (SPX/TCP).

This port is used to receive commands from Information Server.

Installing ServerProtect for NetApp

To install, perform the following steps:

1. Install the Information Server. See *Installing an Information Server* on page 2-16.

2. Install the Normal Server on the Information Server computer. See *Installing a Normal Server from the Setup Program* on page 2-20.

3. Install the Management Console on the Information Server computer. See *Installing the Management Console* on page 2-14. You can install additional Management Consoles on any Windows server or desktop system computer in the network.

Tip: Only one Management Console can manage an Information Server at any given time.

---

4. Update ServerProtect pattern and scan engine files. See *Downloading Updates* on page 3-26 and *Configuring Updates* on page 3-23.

5. Create additional ServerProtect domains to manage your Normal Servers. See *Creating ServerProtect Domains* on page 3-9.

6. Install the remaining Normal Servers using the Management Console. See *Installing a Normal Server from the Management Console* on page 2-23.

Steps 1, 2 and 3 can be executed simultaneously during the initial setup.

Managing ServerProtect Across a Wide Area Network

ServerProtect can be managed from multiple locations across a WAN. However, to ensure proper network performance, Trend Micro suggests that you install Information Servers in the same network domain of a workgroup of the network as the Normal Servers they manage.

Because the Management Console uses TCP/IP to communicate with Information Servers, it's easy to manage ServerProtect from any point inside most company Intranets.

Installing ServerProtect

For a server network system on which ServerProtect has never been installed or already has been uninstalled, it is recommended that the user choose the complete ServerProtect package installation, which includes installing the Management Console, Information Server and the Normal Server. The program installed in this way will guarantee that the ServerProtect be readily operational, and that the installation operation itself be straight forward and smoothly carried out.

This section guides you through the ServerProtect installation process.

Before Installing ServerProtect

As with any server software installation or upgrade, Trend Micro recommends that this activity be performed when the impact to users is minimal; that is, outside business hours and after a full system backup has been completed. Before carrying out a network installation, make sure that the network connections among the related server computers are established.

It is also good practice to install the program on a test server first so that installation issues, if any, can be identified and handled properly before the installation. Before installing ServerProtect, make sure you carefully read the Installation Scenarios section. See *Installation Scenarios* on page 2-5.

Note: You must be logged on with administrator privileges in order to install ServerProtect.

Installing the Complete ServerProtect Package

To install the complete ServerProtect package, including the Management Console, Information Server and the Normal Server, execute the setup program on one or more Windows platform computers.

To install the complete ServerProtect package:

1. Insert the Enterprise CD-ROM and run SETUP.EXE. The ServerProtect **Welcome** screen appears.
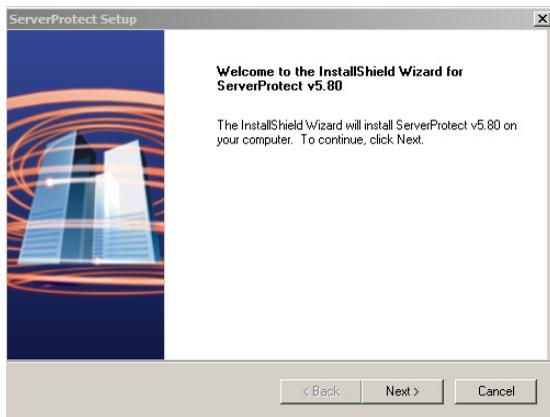
FIGURE 2-4.   ServerProtect Welcome screen

2. Click **Next**. The **Software License Agreement** screen appears. You must agree to the license conditions to proceed with Setup.
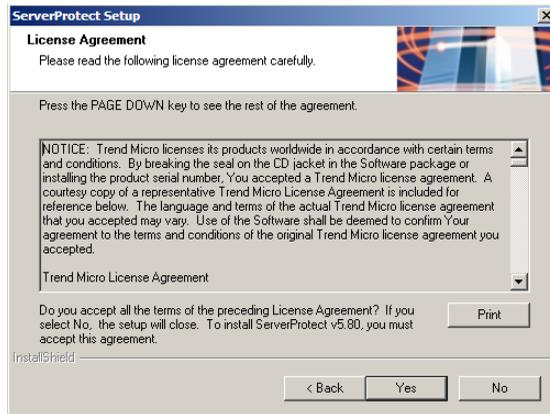
FIGURE 2-5.   Software License Agreement screen

3. Click **Yes**. ServerProtect checks the boot sector of the storage hardware for viruses.
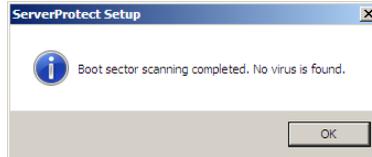
FIGURE 2-6.   Scan Result Information screen

4. Click **OK** to continue. The **User Information** screen appears.

FIGURE 2-7. ServerProtect User Information screen

5. Provide your user information including the product's serial number.

Even with the serial number field left empty, the ServerProtect will still be installed to allow the user enjoy a trial version of the program valid for a 30-day period. If the serial number entered is invalid, the installation program appears a message box, showing "The serial number is incorrect, please try again".

6. Click **Next** to continue. The **Select Components** screen appears.
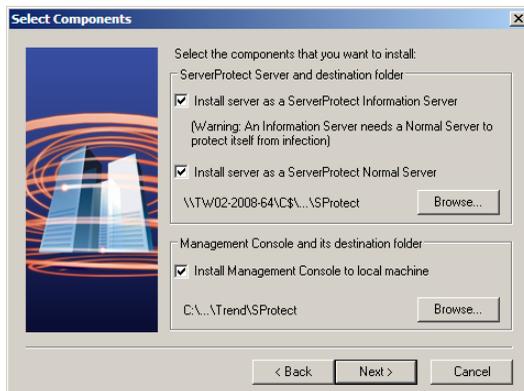
FIGURE 2-8.   ServerProtect Select Components screen

7. Select the check boxes for the components you want to install. Make sure the selection of the components is adequate for the desired setup. You can choose hidden shared storage devices, such as **C$** or **D$**, as destination folders.

    The default installation path is:

    ```
    <drive>:\Program Files\Trend\SProtect
    ```

    Note: To protect the Information Server, Trend Micro recommends that you install a Normal Server on the computer where the Information Server managing is installed.

8. Click **Next**. If you chose to install either a Normal Server or an Information Server, the **Input Logon Information** screen will appear.

Under **Logon Information,** type the appropriate data in the **Domain name**, **User name**, **Password**, and **Confirm Password** fields. Click **Next** to continue.
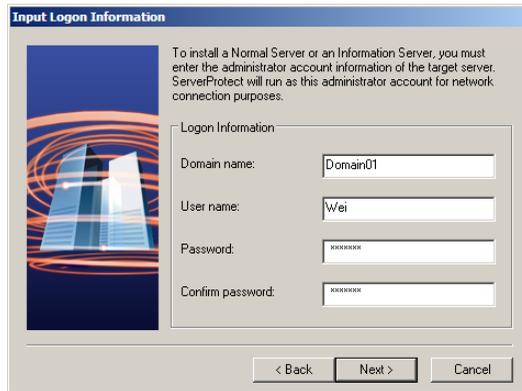
FIGURE 2-9.   Input Logon Information screen

9. Follow the instructions given in the following sections to complete the Installation.

Installing the Management Console

Administrators can remotely manage ServerProtect Normal Servers using the Management Console. The Management Console is the ServerProtect component users interact with; it can be installed on the same computer along with the Information Server and the Normal Server, or on a different computer.

To install the Management Console:

1. Execute the setup program and complete the necessary steps to provide product information.

2. At the **Select Components** screen, select the **Install Management Console** check box. You can change the local installation path by clicking **Browse**. The Management Console must be installed in a Windows Storage Server environment.

Note: Trend Micro does not currently support remote installation of the Management Console.

3. If you want to be the only one to view the ServerProtect program from the Windows Start menu, click **Personal program folder**. Otherwise, click **Common program folder**. Click **OK**. The **Start Copying Files** screen appears.

4. Click **Next** to continue with the setup program. Setup starts copying all program components and starts all services. After all program components have been copied, the **ServerProtect Setup** screen appears.
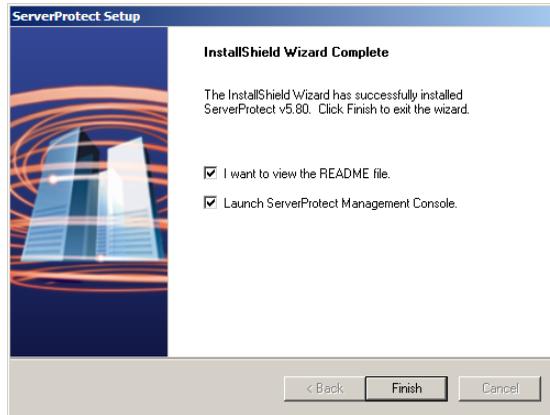
FIGURE 2-10. ServerProtect Setup Complete screen

5. Click **Finish**. The **Select an Information Server** screen appears.
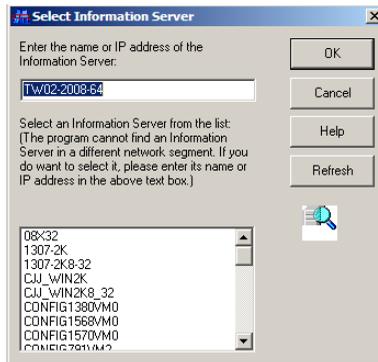
FIGURE 2-11. Select an Information Server screen

6. Select the Information Server that the Management Console will control. Do one of the following:

- Select a server from the list.
- Provide the name of the server.
- Provide the IP address of the server.

Note: If an Information Server resides on a different network segment from the one where the Management Console is installed, the server will not appear in the list.

---

7. Click **OK** to save your changes or click **Cancel** to close the screen without saving.

Installing an Information Server

The Information Server carries out the commands issued by the Management Console and manages Normal Servers hosted by its Information Server domain(s).

To install the Information Server:

1. Execute the setup program and complete the necessary steps to provide product information.
2. Select the **Install server as a ServerProtect Information Server** check box on the **ServerProtect Select Components** screen. **See** *ServerProtect Select Components screen* on page 2-13

3. Click **Browse** to specify the path where you want to install the Information Server. The **ServerProtect Install Path Selection** screen appears.
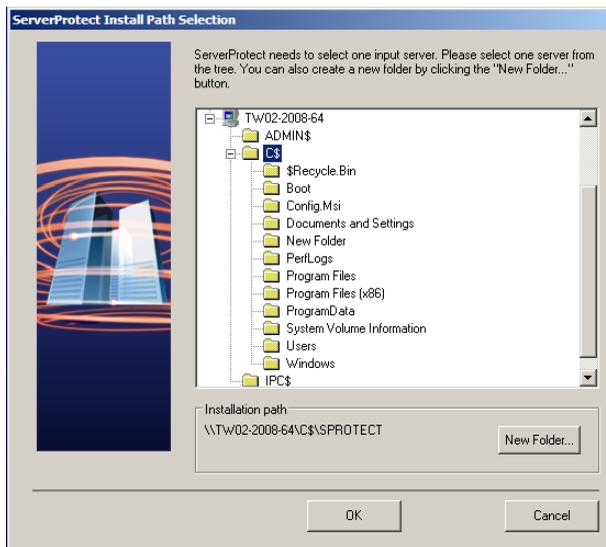
FIGURE 2-12.   ServerProtect Install Path Selection screen

4. Double-click the target server and choose the installation path for ServerProtect Information Server files. Click **New Folder** if installation needs to be installed in a new folder. Click **OK** to bring back the **ServerProtect Select Components** screen. See *ServerProtect Select Components screen* on page 2-13.

5. Click **Next**. The **Input Logon Information** screen appears. Under **Logon Information,** type the valid data in the fields of **Domain name**, **User name**,

Password, and **Confirm Password** and click **Next**. The ServerProtect **Setup Information Server** screen appears.
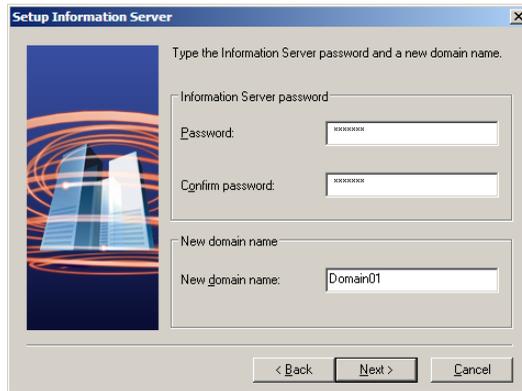
FIGURE 2-13. ServerProtect Setup Information Server screen

6. Provide a password and make the confirmation as requested. This prevents unauthorized access to this Information Server from either the Management Console or the setup program.

7. Click **Next**. The **Start Copying Files** screen appears. Verify the information listed on the screen.

8. Click **Next** to continue with the setup program. ServerProtect now starts copying all program components and starts all services. After all program components have

been copied and all services have started successfully, the **ServerProtect Setup** screen appears.
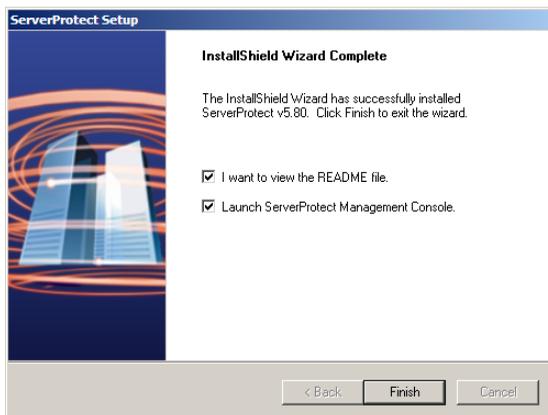
FIGURE 2-14. ServerProtect Setup Complete screen

9. Click **Finish.** The **Question** dialog box appears.
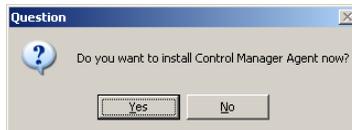
FIGURE 2-15. Question dialog

10. Click **Yes** to the installation of the Control Manager Agent program is needed; otherwise, click **No** to conclude the installation program.

Installing a Normal Server

Use the setup program the first time you install a Normal Server. After that, use the Management Console to install additional Normal Servers.

Installing a Normal Server from the Setup Program

The setup program allows you to install a Normal Server both locally and remotely to the server network. The installation procedures for separately Normal Server of Microsoft Windows will be presented separately.

To install a Windows Normal Server from the setup program:

1. Execute the setup program and provide the necessary product information.

2. Select the **Install server as a ServerProtect Normal Server** check box on the **Select Components** screen. See *ServerProtect Select Components screen* on page 2-13. Click **Browse** to locate the target server and folder where you want to install a Normal Server. The **ServerProtect Install Path Selection** screen appears.
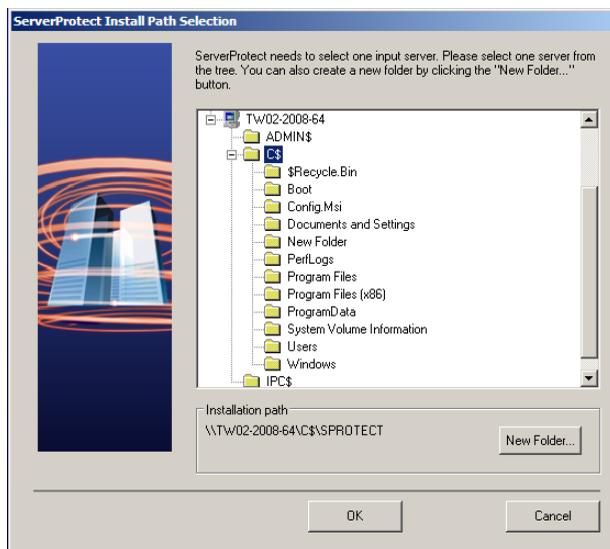
FIGURE 2-16. ServerProtect Install Path Selection screen with Windows Server

3. Click the appropriate network to expand the directory tree and select a target server.

4. Double-click on the target server. In the **Enter Password** screen subsequently appears, type an administrator user name and password and click **OK**. The target server's local drives appear on the tree.

FIGURE **2-17. ServerProtect Target Server Logon screen**

5. Select the installation path for the Normal Server. Click **New Folder** if installation needs to be installed in a new folder. Click **OK** to continue.

6. Click **Next** in the **ServerProtect Select Components** screen. The **Input Logon Information** screen appears.

7. Under **Logon Information**, type the appropriate data next to the **Domain name**, **User name**, **Password**, and **Confirm Password** fields.

8. Click **Next**, the **Select Information Server** screen appears.
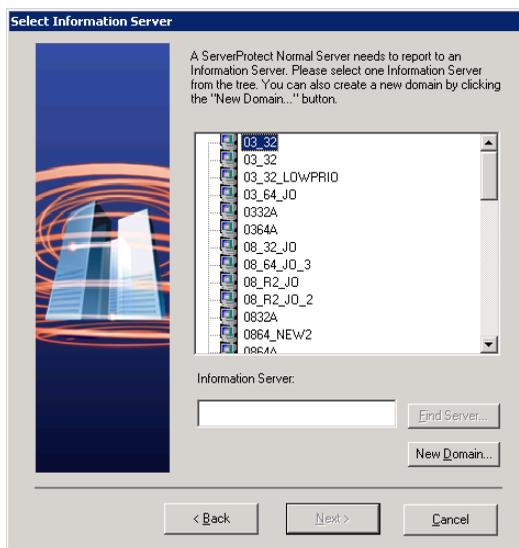
FIGURE **2-18. Select Information Server screen**

9. To locate the Information Server, do one of the following:

   • Type the name or IP address of the Information Server in the text box below the tree. Click **Find Server**.

   • Double-click the target server for the Information Server in the browser tree.

10. Click **New Domain** if a new ServerProtect domain is needed to host the Normal Server.

Note: If an Information Server resides on a network different from the one the Normal Server does, the server does not show up in the list. To locate the Information Server in this case, type the server name or the IP address in the **Information Server** fields.

---

11. Type the Information Server password and click **OK**. This password was assigned during Information Server installation.
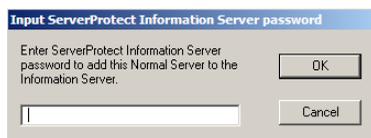
FIGURE 2-19. Input ServerProtect Information Password dialog

Click **Next**. The **Start Copying Files** dialog appears. Verify the information listed on the screen.

12. Click **Next** to continue with the setup program. ServerProtect now starts copying all program components and starts all services. After all program components have been copied and all services have started successfully, the **Setup Complete** screen appears.

13. Click **Finish**. An icon () will be added to your Windows taskbar, notifying you that the scanner is on.

Installing a Normal Server from the Management Console

It can be assumed at this point that the Information Server on which the Management Console is logged is already managing at least one Normal Server. This server will be used as a source for installing the new Normal Server, so it must be of the same type as the one that needs to be installed. For example, a Windows Storage server requires a Windows storage type server as its source. The system will select a Normal Server of the same type as the default source server if it is the one existing in the domain.

To install a Microsoft Windows Normal Server from the Management Console:

Note: While installing a Windows Normal Server from the Management Console, ensure that the operating system of the source and the target servers are of the same platform. For example, if the operating system of the source server is 32-bit, then the operating system of the target server should also be 32-bit.

Ensure that ServerProtect was not installed on the target server before.

1. From the domain browser tree, select the domain to which you want to add a server. Do one of the following:

    • Select **Domain > Install New SPNT(s)** from the main menu.

    • Right-click the domain that you selected in the previous step and click **Install New SPNT(s).**

    The **Select a Source Server** screen opens.

2. Select an existing Windows Normal Server from the list box, and then click **OK**. A confirmation screen appears. Click **OK** to bring up the **Add Server(s) to Domain** screen.

3. Do one of the following to add a server to the domain:

    • Select the server name in the left list box

    • Type the server name in **Server name.**

    Click **Add** to enter the server name into the right list box.

4. Repeat step 3 until the right list box displays all the servers that you want to add into the new domain. To remove a server previously added, highlight the name in the right list box and click **Remove**. Click **Remove All** to remove all those servers listed in the right list box.

5. Click **OK** to save the changes or click **Cancel** to close the screen without adding a server.

Deploying through Microsoft SMS

You can install ServerProtect using Microsoft Systems Management Server (SMS) onto a Windows Server platform.

Note: You must install the Microsoft SMS software on your Windows Server computer before using it to deploy any client software.

The deployment procedures listed as follows illustrate how to deploy ServerProtect through Microsoft SMS.

To deploy ServerProtect through Microsoft SMS:

1. Open the Microsoft SMS Administrator.

2. Click **Packages** on the SMS Administrator's icon bar.

3. Click **Action** > **New** > **Package From Definition** on the main menu. The **Welcome to the Create Package from Definition Wizard** screen appears.

FIGURE 2-20. Create Package from Definition Wizard screen

4. Click **Next**. The **Package Definition** screen appears.
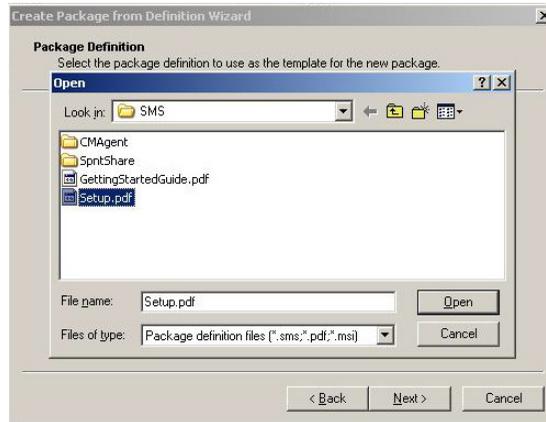
FIGURE 2-21. File Browser dialog

5. Click **Browse** to locate the package description file (PDF) for installing ServerProtect. Select the PDF file and click **Open**.

The default directory for ServerProtect software:

```
<drive>:\Program Files\Trend\SProtect\SMS\
```

The description of the PDF file will be displayed as 'ServerProtect' in the **Package Definition** screen.

FIGURE 2-22.   Create Package from Definition Wizard

6.   Click Next, the Source Files screen appears.
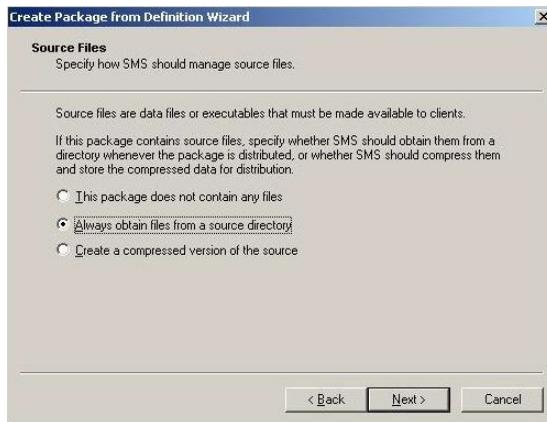
FIGURE 2-23.   Source Files screen

7. Select the **Always obtain files from a source directory** option and click **Next**. The **Source Directory** screen appears.
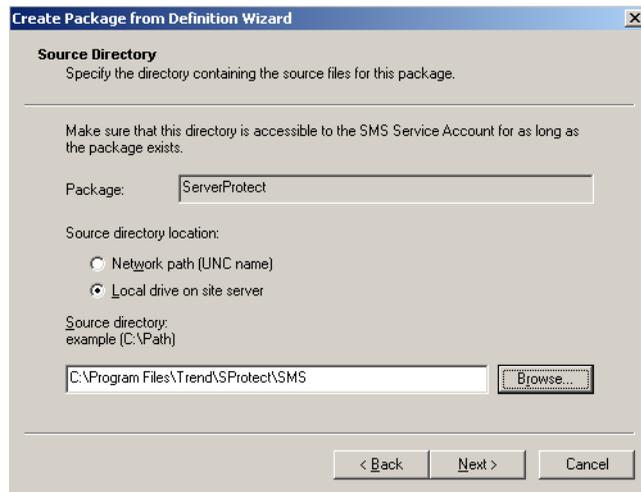
FIGURE 2-24. Source Directory screen

8. Select the **Local drive on site server** option.

9. Click **Browse** to locate the directory where the package description file (PDF) for installing ServerProtect is. Select the directory and click **Next**. The **Completing the Create Package from Definition Wizard** screen appears.
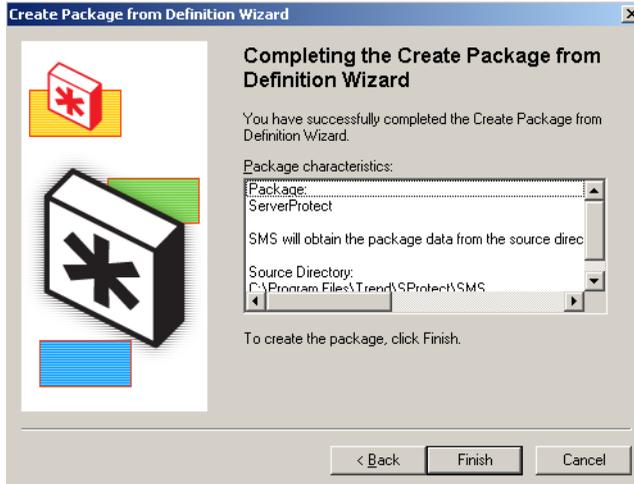
FIGURE 2-25. Completing the Create Package from Definition Wizard screen

10. Click **Finish** to create the package.

11. To select the servers/workstations, from where you want to install the software, browse to **Packages** > **ServerProtect** > **Distribution Points** in the SMS Administrator's explorer tree.
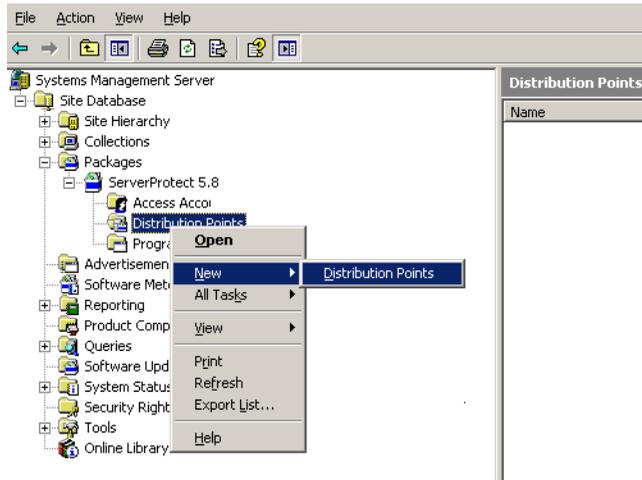
FIGURE 2-26. SMS Administrator screen

12. Right-click **Distribution Points** and select **New** > **Distribution Points**. The **Copy Package** screen appears.
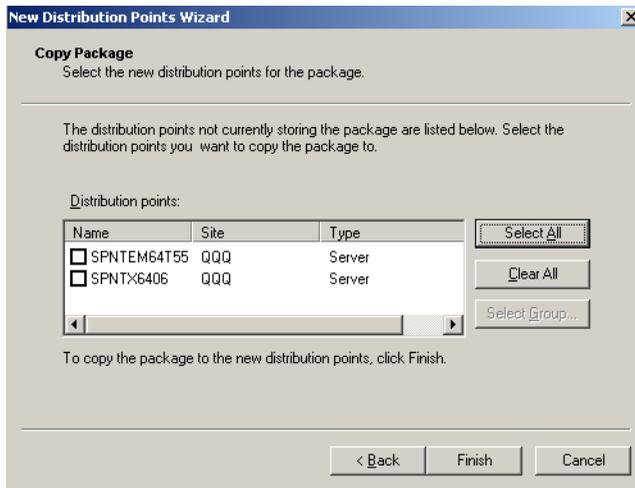
FIGURE 2-27. Copy Package screen

13. Select the distribution point and click **Finish** to copy the package to the distribution point.

14. To install ServerProtect in multiple servers/workstations, right-click **Advertisements** in the SMS Administrator's explorer tree.

15. Select **New** > **Advertisement**. The **Advertisement Properties** screen appears.
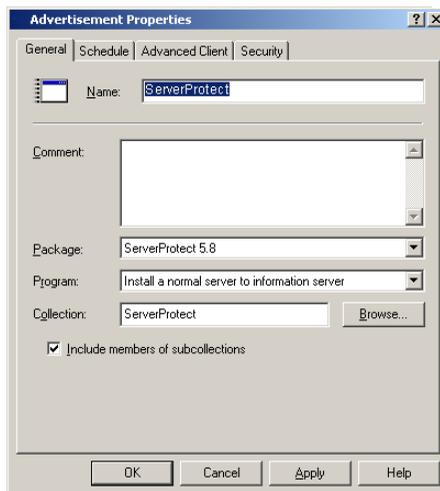
FIGURE 2-28. Advertisement Properties screen

16. Under **General** do the following:

    a. In the **Name** text box, type an appropriate advertisement name.

    b. In the **Package** list**,** select the package you want to deploy.

    c. In the **Program** list, select the program you want to deploy.

    d. Click **Browse** to locate and select the **Collection** of servers/workstations, where you want to deploy the program.

17. Click **OK** to deploy the program in the servers and workstations collection.

Installing ServerProtect in Silent Mode

Installing ServerProtect in silent mode can be quite useful to remotely install Normal Servers under Microsoft Window environment.

To install ServerProtect in silent mode for Windows Servers:

1. Install an Information Server. See *Installing an Information Server* on page 2-16.

2. Locate the SMS folder in the default installation path, and share it. Make sure the target servers you want to install as Normal Servers can access the folder. If you want to perform more than one silent installation, map the SMS folder on the target servers.

3. At the target server, open a command prompt, go to the SMS folder or drive that is mapped to the folder, and then enter the following command:

```
<drive>:\setup -SMS -s -m"SPNAF"
```

Example:

a. At the target server, map the SMS folder to drive "M".

b. Open a command prompt.

c. Go to drive M: by typing "M:".

d. Type the following:

```
M:\setup -SMS -s -m"SPNAF"
```

e. Press **Enter**.

Silent install will proceed and the target server will be registered with the Information Server.

For a silent installation, Normal Servers are installed in the "SMS" domain. There is no way to change the domain name during the silent installation. You can, however, rename the SMS domain after all the Normal Servers have been installed.

You can also specify a path to which ServerProtect is installed. For example, to install ServerProtect to the path "D:\Utility\AntiVirus\SProtect" do the following:

1. Locate the Setup.ini file in the source folder.

2. Add the following lines:

```
[CommonSection]

ServerTargetUNCPath=D$\Utility\AntiVirus\SProtect
```

Where:

ServerTargetUNCPath: Sets the location where the Normal Server is installed.

To license the installed Normal Server, add the following lines to the Setup.ini file in the source folder.

```
[CommonSection]

ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

Where:

XXXX-XXXX-XXXX-XXXX-XXXX: Represents the legal serial number.

You may not be able to register a Normal Server under the "SMS" domain due to the use of a domain controller on the Information Server. To resolve this issue, configure an IP address before using silent install.

To configure an IP address, do the following:

1. Go to the Setup.ini file in the SMS folder.

2. Replace the host name with its IP address next to **AgentName** then save the file.

Removing ServerProtect

ServerProtect's three components can be removed either together or separately. Individual removal is discussed in the following sections.

Removing a Normal Server

There are two ways to remove a Normal Server:

To remove a Normal Server remotely:

1. Select the Normal Servers intended for removal from the Management Console.

2. From the main menu, navigate from **Domain** > **Uninstall ServerProtect**.

To remove a Normal Server locally:

1. Navigate from Windows Desktop's **Start** button > **Settings** > **Control Panel** > **Add/Remove Programs**.

2. Select the Normal Servers intended for removal and click the **Remove** button.

Removing an Information Server

The Information Server Service can only be removed locally.

To remove an Information Server for the Windows Server family platform:

1. Click **Start** > **Control Panel** > **Add/Remove Programs**.

2. Click **ServerProtect Information Server,** and then click **Remove**.

Removing the Management Console

The Management Console can only be removed locally.

To remove the ServerProtect Management Console from the Windows Server:

1. Click **Start** > **Control Panel** > **Add/Remove Programs**.

2. Click **ServerProtect Management Console,** and then click **Remove**.

Chapter 3

Managing ServerProtect

This chapter covers the essential tools for managing ServerProtect. Additional management tools are explained in the online help of the Management Console.

The topics included in this chapter are:

Using the Management Console

ServerProtect allows you to manage virus protection over multiple Microsoft Windows network servers from a single, portable Management Console. It is password protected to ensure that only authorized users can change the settings of ServerProtect.

Opening the Management Console

The Management Console can run on any 32-bit or 64-bit Windows server or desktop computer on the network.

To run the Management Console:

1. Click **Start** > **Trend ServerProtect Management Console**. The system prompts for the administration password to log on to the selected Information Server.

FIGURE 3-29. Trend ServerProtect Management Console Logon dialog

---

> **Note:** If you are managing more than one Information Server, you will be prompted to choose one from a list before proceeding.

---

2. Provide the valid password which is designated during the course of the Information Server installation. Click **OK** to continue. Note that the password is case-sensitive and that only one Information Server can be logged on at any given time.

3. If it is the first time for the ServerProtect to run on the system, a message box appears, indicating that new updates may be available on the Trend Micro AcitveUpdate Server to download and deploy. It is highly recommend that an update be performed before using ServerProtect virus scan utilities on the network.

The Main Window View of the Management Console

The ServerProtect Management Console has an intuitive user interface that provides easy access to all the functions you need to configure and manage ServerProtect.
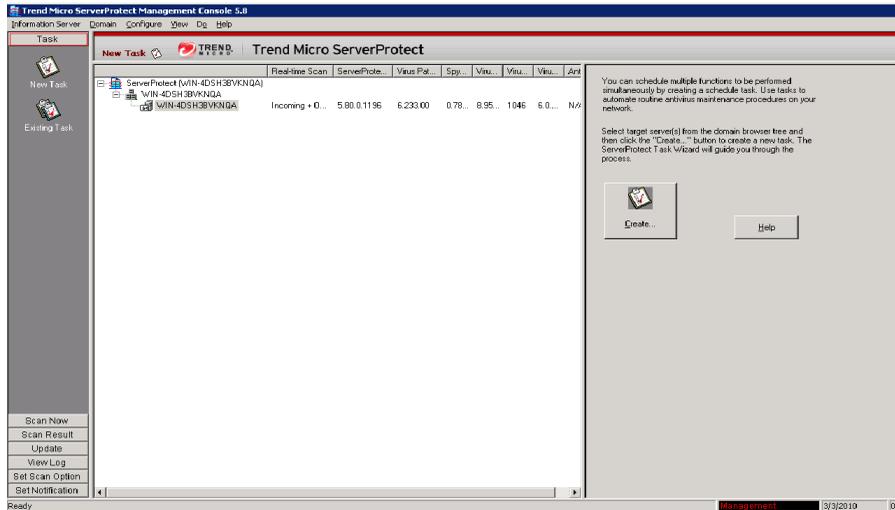
The Management Console has the following components:

- **Main Menu:** located below the title bar; contains six submenus, with each providing menu items for users to choose

- **Side Bar:** located on the left side of the application dialog, below the **Main Menu**; contains seven items, with each having additional options to choose

- **Domain Browser Tree:** located on the right of the **Side Bar** and below the **Main Menu**; the tree view presents the ServerProtect organization, including the **Information Server, Domain** elements, and **Normal Server**s

- **Configuration Area:** has a light gray background color on the right side of the main Window; provides information and UI elements to configure the virus scan and log report systems

Main Menu

The Main menu at the top of the screen includes:

- **Information Server**: Information Server configuration; for example, back up or restore the Information Server or move it on the network
- **Domain**: change the domain and server organization shown on the domain browser tree
- **Configure**: modify the scanning and log file configuration or set the console refresh frequency
- **View**: view ServerProtect log files, scan results, and the Trend Micro Virus Encyclopedia
- **Do**:
    - **Create Task / Existing Task:** create or modify tasks
    - **Scan Now:** perform on-demand scans
    - **Update / Rollback:** update or roll back various ServerProtect antivirus elements
    - **Update Serial Number:** type a new serial number to replace an expired one
    - **Change Password:** change the IS password
    - **Find Domain:** find domains or servers
    - **Connect to Server with STOP Sign:** use when the Normal Server is running and managed by one Information Server, but displays **STOP** in the Management Console
    - **Submit File:** submit a suspicious file or a file that cannot be cleaned to the virus doctor at Trend Micro free of charge; virus doctor will clean the file and return it to you via e-mail
    - **Create Debug Info:** manage log files that contain detailed debugging information and send them to Trend Micro technical support engineers for assistance
    - **Send Feature Request:** use to send requests for new features that you would like to see added to ServerProtect
- **Help**: open the Online Help system or view ServerProtect product information

Side Bar

The side bar is on the left side of the ServerProtect screen and includes seven groups of items. It provides shortcuts to different functional areas of the program.

Task Group

New Task: create a new task

Existing Task: view, run, modify, or delete an existing task

Scan Group

Scan Now: configure a manual virus scan

Scan Result Group

Real-time Scan: view a real-time scan result

Scan Now: view manual scan result

Task Scan: view task scan result

Update Group

Update: download and deploy updates to the Normal Servers

Rollback: roll back to a previous deployment

View Log Group

View Log: view historical information about antivirus events that have occurred on the network

Set Scan Action Group

Real-time Scan: configure a real-time virus scan

Exclusion List: define files, directories, or viruses to be ignored by the ServerProtect virus scanning engine

Deny Write List: prevent certain files or directories from modification

Notification Group

Standard Notification: configure a standard alert when the default condition is detected on the server

Outbreak Notification: configure an outbreak alert when many virus events occur over a relatively short period of time

Domain Browser Tree

The browser tree displays the network components that your software is protecting and includes a root (the ServerProtect product icon), branches (domains), and nodes (the ServerProtect Normal Servers). There are four main visible items in the domain browser tree:

• Header

• Information Server

• Domain

• Normal Server

Header

The column fields above the domain browser tree display useful information, such as the computer's operating system, virus pattern, scan engine, program versions, real-time scan direction, and so on.

Right-click tree icons in the ServerProtect console to make configuration changes to the selected components. The frame that contains the domain browser tree can be resized.

Information Server

An Information Server is the server that handles key information and communication for domains. In addition, the Information Server links domains together.

 An Information Server

Domain

Domains are groupings of servers on your ServerProtect network. Normal Servers that belong to a domain are managed together. ServerProtect domains are different from Windows domains.

 A ServerProtect domain

 A ServerProtect domain that includes an infected Normal Server

3-7

Normal Server

The Normal Server can be any server in which ServerProtect is installed on a network. In the ServerProtect architecture, a Normal Server is managed by the Information Server.

A Normal Server of 32-bit Microsoft Windows Server type.

A Normal Server of 64-bit Microsoft Windows Server type.

An infected Normal Server of 32-bit Microsoft Windows Server type.

An infected Normal Server of 64-bit Microsoft Windows Server type.

A Normal Server that has been disconnected or its service has been disabled.

A Normal Server of 32-bit Microsoft Windows Server type in Outbreak. Prevention Policy mode.

A Normal Server of 64-bit Microsoft Windows Server type in Outbreak. Prevention Policy mode.

An infected Normal Server of 32-bit Microsoft Windows in Outbreak Prevention Policy mode.

An infected Normal Server of 64-bit Microsoft Windows in Outbreak Prevention Policy mode.

Configuration Area

On the right side of the ServerProtect screen is the configuration area, where you can type configuration data and view information about your corporate network.
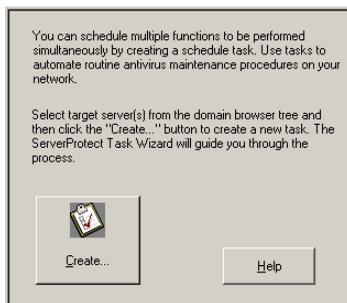
FIGURE 3-31.   Configuration Area

Managing ServerProtect Domains

ServerProtect domains are virtual groupings of Normal Servers used to simplify their identification and management. You can create, rename, or delete domains according to the needs of your network.

Note: If one of the servers in a domain is infected, the domain icon will change and the infected server's icon will appear with a flame. This is to remind you to scan the infected server and prevent the virus from spreading throughout your network. To eliminate the infection icon(s), you need to purge all log entries under **Scan Result** in the Management Console, or open all these log entries.

Creating ServerProtect Domains

After creating a default domain through the ServerProtect installation program you can create a domain from the Management Console.

The maximum length of a domain name is 50 single-byte characters or 25 double-byte characters (for Chinese, Japanese, or Korean characters).

To create a ServerProtect domain:

1. Do one of the following:

    •   Select the Information Server you want to add a domain. Navigate from the main menu **Domain** > **Add New Domain**.

    •   Right-click the Information Server icon on the domain browser tree and then click **Add New Domain**.

    The **Create New Domain** screen appears.
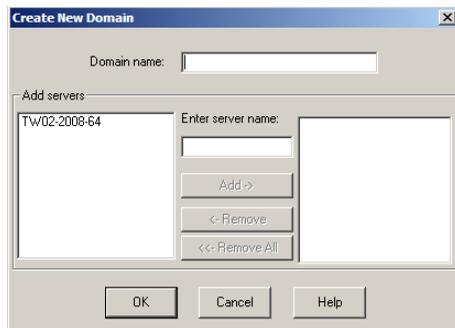
FIGURE 3-32. Create New Domain(s) screen

2. Type a name in the **Domain name** field.

3. Identify the servers that you want to add to the domain. Do one of the following:

    •   Select a server from the list on the left of the screen.

    •   Type the server name in the **Enter server name** field.

4. Click **Add**.

5. Repeat steps 3 and 4 until the list on the right displays all the servers that you want to add in the new domain. To remove a server, select it in the list on the right and click **Remove**. Click **Remove All** to delete all the servers from the list on the right.

6. Click **OK** to save your changes or click **Cancel** to close the dialog without creating a new domain.

Renaming ServerProtect Domains

A domain with your server's name is created as the default domain during ServerProtect installation. You can change the name of any existing domain from the Management Console.

To rename a ServerProtect domain:

1. Select the domain you want to rename in the domain browser tree.
2. Do one of the following:
   - Right-click the selected domain, and then click **Rename Domain**.
   - Select **Domain** > **Rename Domain** on the main menu.
   - Press the **F2** key on the keyboard.

   The **Rename a Domain** dialog appears.
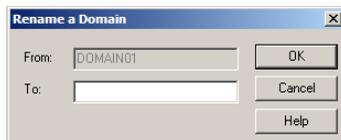
FIGURE 3-33.   Rename a Domain dialog

3. Type the new domain name in the **To** text box and then click **OK**. Click **Cancel** to close the dialog without saving.

Deleting ServerProtect Domains

You can delete empty domains (domains that do not include any Normal Servers) you no longer need. You cannot delete a domain if it contains any Normal Servers.

To delete a ServerProtect domain:

1. Select the domain that you want to delete on the domain browser tree.
2. Do one of the following:
   - Right-click the domain and then click **Delete Domain**.
   - Click **Domain** > **Delete Domain** on the main menu.
   - Press the **Delete** key of the keyboard.

Note: You cannot delete a domain if it contains any Normal Servers.

Moving Normal Servers between Domains

To improve management, sometimes you need to move (remove and add) Normal Servers from one domain to another. Select Normal Server(s) under one domain from the domain browser tree, then drag and drop between domains.

Alternatively, you can move a Normal Server when you create a ServerProtect domain. See *Creating ServerProtect Domains* on page 3-9.

Managing Information Servers

The Information Server stores and delivers data to and from the Normal Servers. In a Windows Server network, the Normal Servers deliver their alert notifications to the Windows server.

Because an Information Server is simply a delivery system for information, the number of servers it can manage is, theoretically, only limited by the available bandwidth.

Tip: For large networks such as WANs, Trend Micro recommends that you install an Information Server in each network segment. This will reduce the impact on traffic.

Selecting Information Servers

Management Consoles can switch between Information Servers. However, only one Management Console can log on to an Information Server at any time. If you are not able to log on to an Information Server, verify whether another Management Console is connected to it.

To select an Information Server:

1. Click **Information Server** > **Select Information Server** on the main menu. The **Select Information Server** screen appears.
2. Do one of the following:

- Type the name or IP address of the Information Server.
- Select the Information Server from the list.

Note that if more than one network interface cards (NIC) are installed on the computer, only those Information Servers that connect to the primary NIC are visible in the list box dialog. To refresh the view of servers in the list, click **Refresh** button.
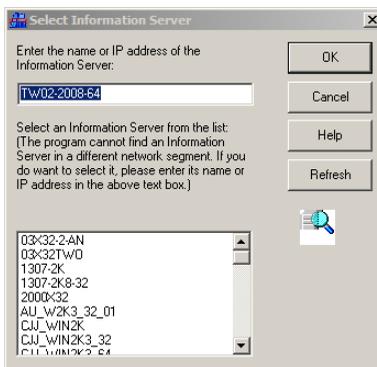
FIGURE 3-34.   Trend ServerProtect Management Console dialog

3. Click **OK** to save your changes or click **Cancel** to close the dialog without saving.

Managing Normal Servers

In the ServerProtect architecture, the Normal Server is the first line of defense against viruses, and is managed by an Information Server. It is at the bottom of the three-tier ServerProtect structure. This section explains how to manage Normal Servers.

Moving a Normal Server between Domains

To move a Normal Server from one ServerProtect domain to another, select a Normal Server in the domain browser tree, then drag and drop it between domains.

Moving a Normal Server between Information Servers

ServerProtect allows you to move a Normal Server from one Information Server to another. This feature is particularly useful to reduce the load on the Information Server.

To move a Normal Server between Information Servers:

Note: You cannot use the **Move NS(s) to Another IS** function to move a previous version of ServerProtect Normal Server to the ServerProtect 5.8 Information Server.

1. Do one of the following:
   - Right-click the Normal Server that you want to move and then click **Move NS(s) to Another IS**.
   - Select the Normal Server that you want to move and then click **Domain** > **Move NS(s) to Another IS** in the main menu.The **Select Destination Information Server** screen appears.
2. Select the destination Information Server and submit it by clicking on the **OK** button. A dialog box **Move NS(s) to Another IS** dialog box appears.
3. Type **User Name/Password** or **GUID** with proper values and click **OK**.

Managing NetApp in Scan Server

A Scan Server can protect multiple NetApp Filers at the same time. Use the ServerProtect Management Console to conveniently add NetApp Filers to a Scan Server. You can also assign several Scan Servers to individual NetApp Filers for load balancing. See *Using Multiple Scan Servers for Single NetApp Filer* on page 3-16.

Note: In the ServerProtect documentation, the Scan Server is called "Normal Server". However, this document uses the term "Scan Server" to describe the machines in Information Server domains that protect the NetApp Filers.

Adding NetApp Filer to Scan Server

To add a NetApp Filer in ServerProtect for NetApp, you need the following:

1. An account on the NetApp Filer with backup operator privileges or above

2. NetApp Filer name or IP address

3. NetApp Filer logon credentials (user name, password)

To add a NetApp Filer:

1. Right-click a Normal Server, and then select **Filer List** on the domain browser tree. The **Filer List** screen appears.

2. Click **Add**. The **Add Filer** screen appears.
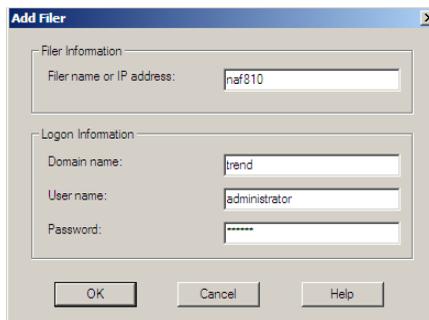
FIGURE 3-35. Add Filer Screen

3. Do the following:
    • In the **Filer name or IP address** text box, type the name or IP address of the NetApp Filer.
    • In the **Domain name** text box, type the name of the domain where the NetApp Filer is located.

Note: The domain name refers to the Windows domain in which NetApp Filers will authenticate registered users.

    • In the **User name** and **Password** text box, type your NetApp Filer logon credentials (requires backup operator or above privileges)

4. Click **OK**.

Note: Scan Server must be located in the same domain as the BlueArc Storage System to correctly support the virus scan option.

Note: If the server computer, on which ServerProtect is to be installed, is running Windows Server 2008, add the Filer and the Scan Server into certain specified domain, and add their IP addresses in Forward Lookup and Reverse Lookup zones.

Moreover, if the Filer and Scan Server are in dfferent domains, you must add and the two domains in the Trust list, by creating domain Trust.

Using Multiple Scan Servers for Single NetApp Filer

ServerProtect for NetApp provides a fully scalable enterprise antivirus solution for organizations using NetApp Filers.

If there is a large volume of incoming files to the NetApp Filer, adding and registering multiple Scan Servers with the NetApp Filer evenly distributes the workload among the registered Scan Servers.

NetApp Filers send files to Scan Servers in "round-robin" fashion. For example, if you have three Scan Servers and the NetApp Filer has four incoming files, the first Scan Server scans the first file, the second Scan Server scans the second file, the third Scan Server scans the third file, the first Scan Server scans the fourth file, and so on.

This even distribution of the workload reduces the loading of Scan Servers (load balancing).

The procedure for adding additional Scan Servers to a NetApp Filer is identical to the procedure for adding Normal Servers in ServerProtect. See *Installing a Normal Server* on page 2-19.

To confirm that multiple Scan Servers are working for a single NetApp Filer:

1. Open the command prompt for the NetApp Filer that you want to verify.
2. At the command prompt, type:

    netapp> vscan scanners

    The NetApp Filer displays a list of Scan Servers by IP address and NetBIOS name.

Removing a NetApp Filer from Scan Server

In several instances, it may be necessary to remove (delete) a NetApp Filer from a Scan Server. For example, when changing, upgrading, or renaming a NetApp Filer. To remove a NetApp Filer, do the following:

1. Right-click a Scan Server, and then select **Filer List** on the domain browser tree. The **Filer List** screen appears.

2. Select one or more NetApp Filers from the list. To multi-select several NetApp Filers, press the **CTRL** key as you select.

3. Click **Remove**. The **Remove Filer** confirmation screen appears.

4. Click **OK**.

Configuring NetApp Filer Options

This section introduces the necessary information for configuring NetApp Filer related settings from the Management Console.

Updating NetApp Filer Information

Changing a NetApp Filer's system information, will require updating the NetApp Filer logon information in ServerProtect for NetApp. The following information is necessary to update a NetApp Filer's system information in ServerProtect for NetApp:

• An account on the NetApp Filer with backup operator privileges or above

• NetApp Filer name or IP address

• NetApp Filer logon credentials (user name, password)

To update NetApp Filer information:

1. Right-click a Scan Server, and then select **Filer List** on the domain browser tree. The **Filer List** screen appears.

2. Select one or more NetApp Filers from the list. To multi-select several NetApp Filers, press the CTRL key as you select.

3. Click **Logon Info**. The **Logon Information** screen appears.

4. Do the following:

   • In the **Domain name** text box, type the name of the domain where the NetApp Filer is located.

- • In the **User name** and **Password** text box, type your NetApp Filer logon
  credentials (requires backup operator or above privileges)

5. Click **Apply** to update the NetApp Filer information. The **Filer information
    update** confirmation screen appears.
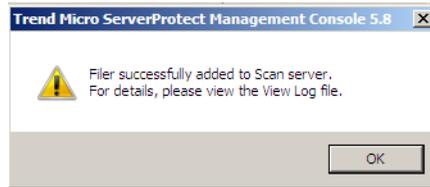
FIGURE 3-36. Filer Information Update Screen

Using Scan Servers as Normal Servers

Although the ideal configuration is to have a machine act primarily as a Scan Server to
protect the NetApp Filer, there may be situations where a Scan Server must also serve as
an organization's Normal Server (file server, data server, etc.).

If you choose to use a Scan Server as a Normal Server, the Normal Server's Real-time
Scan function is enabled by default.

Real-time Scan has the following options:

- • incoming (default)
- • outgoing
- • incoming & outgoing

Note: For the highest level of security set Real-time Scan to **Incoming & outgoing**.
However, if the computer only performs as a Scan Server, you can use the default
setting (**Incoming**).

To set Real-time Scan to Incoming & outgoing, do the following:

1. Select either the Information Server, domain, or a Normal Server (Scan Server) on
    the domain browser tree.

2. Do one of the following:

- • Click **Set Scan Option** > **Real-time Scan** on the side bar

- Click **Configure** > **Scan Options** > **Real-time Scan** on the main menu

The **Real-time Scan configuration** screen appears.

FIGURE 3-37.   Real-time Scan Configuration Screen

3. Under Scan direction, click **Incoming & outgoing**.

4. Click **Apply**.

For more information about Real-time Scan, refer to *Using Real-Time Scan* on page 3-58.

Notifying NetApp Filer clients upon infection

ServerProtect can notify the user and the Network Administrator if a NetApp Filer client has uploaded or accessed an infected file. The notification function is enabled by default.

To notify a user of NetApp Filer client infection do the following:

1. Right-click a Scan Server, and then select **Filer List** on the domain browser tree. The **Filer List** screen appears.

2. Click **Options**. The **Global Filer Options** screen appears.
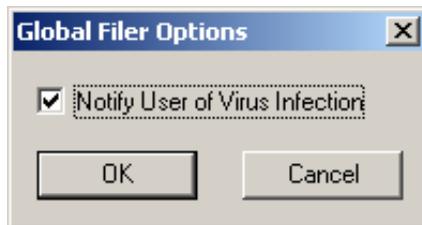
FIGURE 3-38.   Global Filer Options Screen

3. Select **Notify User of Virus Infection**.

4. Click **OK**.

Note: This setting will affect all the NetApp Filers in the Filer list.

Viewing the status of a NetApp Filer

You can see the status of a NetApp Filer through the Management Console. NetApp Filers may appear offline for one of the following reasons:

• The NetApp Filer is shut down or is not responding

• The network is not available

• The NetApp Filer did not successfully register with the Information Server

To view the status of a NetApp Filer do the following:

1. Right-click a Scan Server, and then select **Filer List** on the domain browser tree. The **Filer List** screen appears.
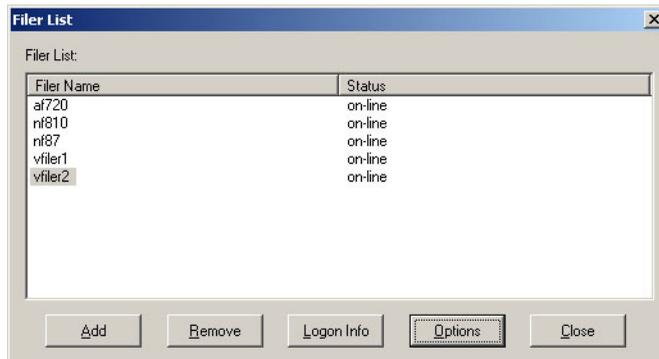
FIGURE 3-39.   Filer List Screen

2. Verify the status of a NetApp Filer by looking at the **Filer name** and **Status** fields in the Filer List. A NetApp Filer may appear as **online** or **offline**.

Configuring NetApp Filer RPC Connection Status Notifications

ServerProtect can notify the network administrator whenever an RPC connection to a NetApp Filer succeeds or fails.

To configure a NetApp Filer RPC connection status notification, do the following:

1. Select the Information Server, domain, or a Normal Server on the domain browser tree.

2. Do one of the following:

- Select **Configure** > **Notifications** > **Standard Alert** from the main menu
- Click **Set Notification**, and then **Standard Alert** on the side bar

3. Select **Filer Rpc Connection Success/Failure**.
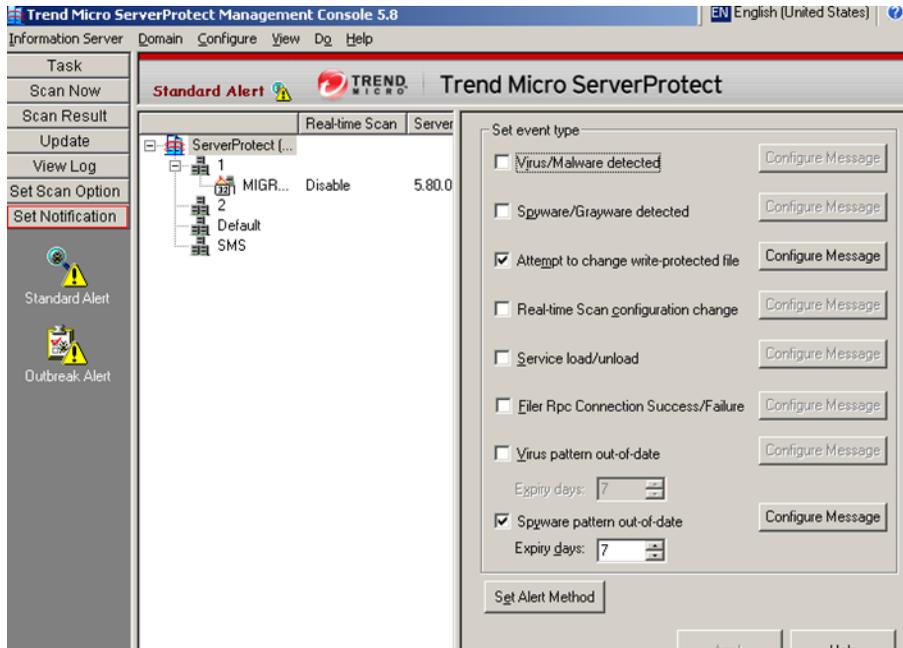
FIGURE 3-40. Standard Alert Configuration Screen

4. Click Configure Message to set up a customized notification message.

Note: For additional information, refer to *Configuring Notification Messages* on page 3-47.

Notifying NetApp Filers of New Update Components

When update downloads new components (scan engine and pattern) to the Scan Server, the Scan Servers will notify NetApp Filers to flush the cache of previously scanned files. This ensures that all files are scanned with the latest virus pattern. Each NetApp Filer will then begin rebuilding the cache of previously scanned files until a new update arrives from the update server.

For more information on downloading updates. See *Downloading Updates* on page 3-26.

Configuring Updates

Trend Micro update server allows you to update ServerProtect components. The update process includes downloading and deploying the updates.

Update Components

The following are the ServerProtect components that you can update:

- **ServerProtect Program**: The application program of the ServerProtect can be downloaded and deployed. The users now have a new option to upgrade the ServerProtect application.

- **Virus pattern file**: Trend Micro antivirus scan software uses a detection method called pattern matching. Files on a computer are examined and compared to the virus pattern file that contains the "electronic fingerprint" of thousands of known computer viruses. If a file on your computer matches one in the pattern file, the antivirus scan software detects it as being infected.

- **Spyware pattern file:** The spyware pattern identifies spyware/grayware in files, programs and modules in memory, Windows registry and URL shortcuts.

- **Scan engine (**for 32-bit and 64-bit Windows and NetWare platform): The scan engine is the software component that performs the actual virus detect operations.

- **Virus Cleanup Engine (for 32-bit and 64-bit Windows)**: the Engine scans for and removes Trojans and Trojan processes. It supports 32-bit and 64-bit platforms.

- **Virus Cleanup Template**: The Virus Cleanup Template is used by the Virus Cleanup Engine to identify Trojan files and processes so the VCE can eliminate them.

- **Anti-Rootkit Driver (for 32-bit Windows only)**: Anti-rootkit Driver is a kernel mode driver used by the Damage Cleanup Engine that provides functionality to bypass any potential redirection by rootkits.

How Updates Work

Figure 3-41 shows how ServerProtect deals with a typical request to download and deploy updates in a ServerProtect network.
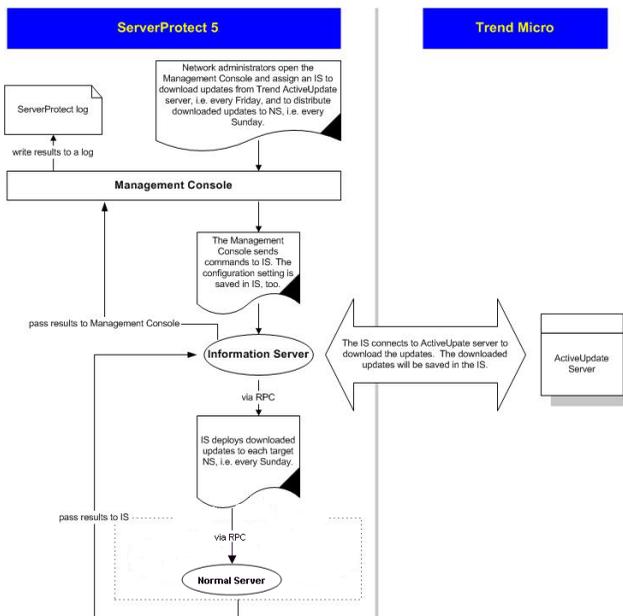
FIGURE 3-41.   How Updates Work

Verifying the Current Version of Files

ServerProtect allows you to check the version of the virus pattern file and scan engine currently used by an Information Server.

To verify the current version do one of the following:

- Click **Update** > **Update** on the side bar.
- Click **Do** > **Update** on the main menu.
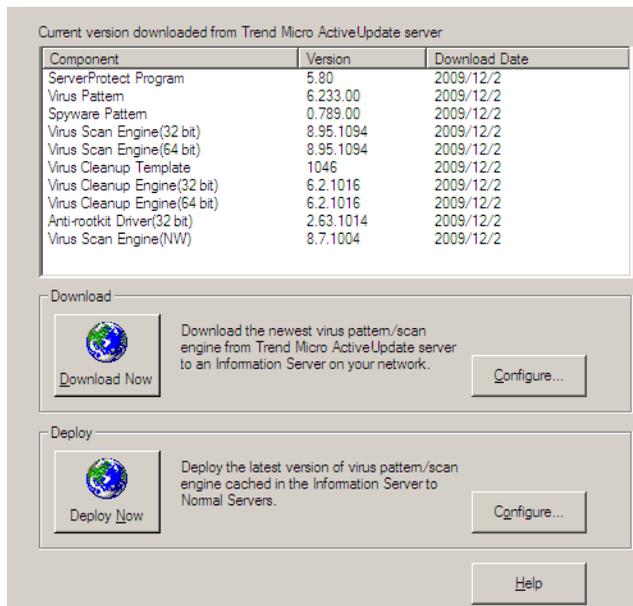
FIGURE 3-42. Trend Micro ServerProtect Update Main Screen

The following version information used by the system are shown at the top of the **Update** screen.

- ServerProtect version.
- Virus Pattern version.
- Spyware Pattern version.
- Virus Scan Engine version (32-bit /64-bit).

- Virus Cleanup Template version.
- Virus Cleanup Engine version (32-bit /64-bit).
- Anti-rootkit Driver version (32-bit only).

After installing ServerProtect for the first time, the version fields are displayed. Updated information will be displayed after you perform a successful update by clicking **Download Now** to download the latest updates from the Trend Micro update server.

Downloading Updates

We recommend that you regularly download updates from Trend Micro update server to ensure continued protection. Trend Micro releases new virus pattern files several times each week. The scan engine files, on the other hand, are updated less frequently.

After downloading updates from the Trend Micro update server, you can designate a network drive to act as a download source (mirror) for other Information Servers on your network. This will avoid redundant downloads.

Downloading updates from a network drive is ideal for large networks (such as Intranets) with multiple Information Servers. Before attempting to download update files from another server, you must make sure the source server has the updated files.

Configuring a Download Source

You can download updated files from Trend Micro update server or copy the files from a location on your network. If you want to copy files from a location on your network, you must create a download source folder.

To set Trend Micro update server as the download source:

1. Do one of the following:
   - Click **Update** > **Update** on the side bar.
   - Click **Do** > **Update** from the main menu.
2. Click **Configure** in the **Download** group to open the **Download Option** dialog.
3. Click **Internet** and then type the following URL to download the update files from the Trend Micro update server:

   ```
   http://spnaf58-p.activeupdate.trendmicro.com/activeupdate
   ```

4. Click **OK**. The downloaded files will be saved in the following directory of the Information Server:

```
<drive>:\Program Files\Trend\SProtect\SpntShare
```

To set a local or network drive as the download source:

1. Do one of the following:
   - Click **Update** > **Update** on the side bar.
   - Click **Do** > **Update** from the main menu.

2. Under **Download**, click **Configure**. The **Download Option** screen appears.

3. Click **From a local or network drive**.

4. Type the UNC path where the files are being kept to download the update files from another server on you network. Use UNC format, rather than mapped drive format to identify the source server.

   For example:

   ```
   \\servername\foldername
   ```

5. Type the **User name** and **Password** to access the source server. The server you are updating from must have previously downloaded a copy of the update files.

6. Click **OK**.

WARNING! **In order to download updates from a local or network drive, you must first create a download source folder. See the procedure listed below.**

To create a download source folder:

1. Execute an update from the Internet by clicking **Download Now**.

2. Do one of the following:
   - Make the SpntShare folder, located under `<drive>:\Program Files\Trend\SProtect\` in the designated Information Server, a shared folder.
   - Create a shared folder on a network server and then copy all the files in the SpntShare folder to the mentioned shared folder.

If you do not select the SpntShare folder as your download source, you need to copy all the files in the SpntShare folder of the designated Information Server to the mentioned shared folder every time you execute an update from the Internet.

Using Download Now

If updated components are available, you can initiate an immediate download of the latest virus pattern files and scan engine files from either the Trend Micro update server or another Information Server on your network.

To use Download Now:

1. Do one of the following:
    *   Click **Update** > **Update** on the side bar.
    *   Click **Do** > **Update** on the main menu.

2. Click **Download Now** on the **Update** main screen. A progress bar appears to show the time remaining until the completion of the update.

Note: Before you use Download Now for the first time, you need to configure the download settings. Failure to do so, could prompt a ***Source network generic failure*** or ***HTTP timeout*** message when you click **Download Now**. See *Configuring Download Settings* on page 3-29.

ServerProtect logs the event in the Information Server logs.

Configuring a Scheduled Download

You can schedule ServerProtect to download the latest update files from Trend Micro or another server on your network.

To configure a scheduled download:

1. Do one of the following:
    *   Click **Update** > **Update** on the side bar.
    *   Click **Do** > **Update** from the main menu.

2. Under **Download,** click **Configure**. The **Download Option** screen appears.

3. Click the **Schedule Setting** tab.
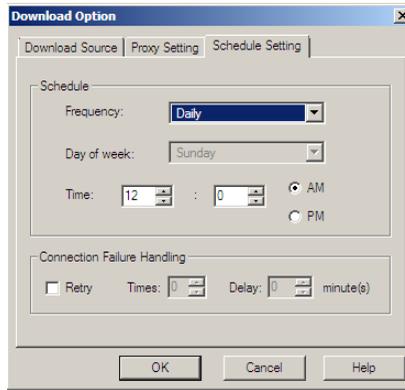
FIGURE **3-43.** **Download Option--Schedule Setting dialog**

4. Under **Schedule** in the **Frequency** list, select download frequency. You can select **None**, **Hourly, Daily** or **Weekly**. If you do not want to schedule a download, select **None**. If you select **Weekly**, from the **Frequency** drop down list, you must also select a **Day of Week**.

5. In the **Time** box, type or select the time when you want to update the components, and then click **AM** or **PM**.

6. Select the **Retry** check box to instruct ServerProtect to attempt to reconnect to the download server if the initial download operation is unsuccessful. In the **Times** and **Delay** boxes, type or select the number of times and the delay you want between each retry.

7. Click **OK**. The downloaded files will be saved under the following directory:

   `\Trend\SProtect\SpntShare`

Configuring Download Settings

The following steps describe how to download the update files

To configure the download settings:

1. Do one of the following:
   - Click **Update** > **Update** on the side bar.

- Click **Do** > **Update** on the main menu.

2. Click **Configure** on the **Update** screen to change your download configuration. The **Download Option** dialog appears.
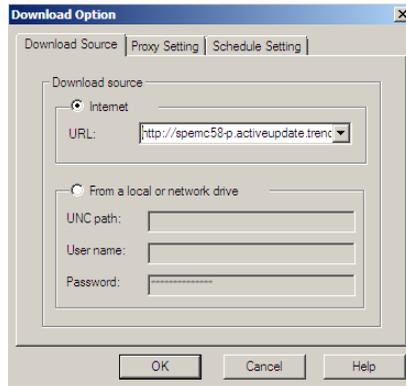
FIGURE 3-44. Download Option dialog

Configuring the Proxy Server Settings

You can configure ServerProtect to use your proxy server settings while connected to the Internet.

To configure a proxy server setting:

1. Choose one of the following:
   - Click **Update** > **Update** on the side bar.
   - Click **Do** > **Update** from the main menu.

2. Under **Download,** click **Configure**. The **Download Option** dialog appears.

3. Click the **Proxy Setting** tab.

FIGURE 3-45.   Download Option--Proxy Setting dialog

4. Select the **Connect to the Internet through a proxy server** check box.

5. In the **Protocol type** list**,** click the protocol used for downloading. The protocols supported are: HTTP and SOCK4.

6. Under **Proxy Setting** do the following**:**

    • In the **Proxy Server** and **Port no** text boxes, type the name of the proxy server and the port number used.

    • In the **User name** and **Password** text boxes, type the appropriate information for the proxy server.

7. Click **OK.**

Deploying Updates

When an Information Server deploys updates to Normal Servers, it sends commands to each Normal Server, requesting them to obtain a copy of the updates. ServerProtect records both the connection and deployment process in a log file.

Configuring Deploy Now

The **Deploy Now** function is used to deploy the updates saved in an Information Server to other Normal Servers.

To deploy an update:

1. Do one of the following:

   • Click **Update** > **Update** on the side bar.

   • Click **Do** > **Update** from the main menu.

2. Click **Deploy Now**. A confirmation dialog appears. Click **Yes** to proceed with the manual update deployment. The **Deploy** dialog appears.
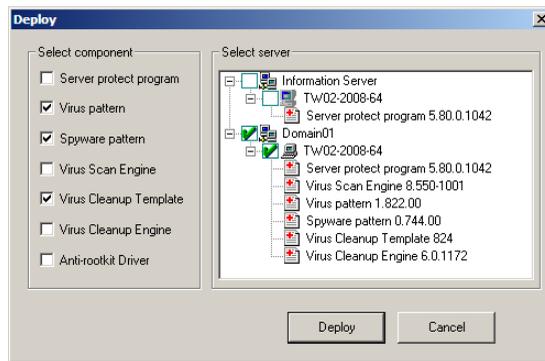
FIGURE 3-46. Deploy dialog

The check boxes in the **Select component** group present those components ready to be deployed to the Normal Servers. **Virus pattern**, **Spyware** and **Virus cleanup Template** are selected at the application initiation stage as part of default configuration settings. In the **Select server** pane, the version information of each downloaded ServerProtect antivirus elements is shown in the tree view UI element. For a 64-bit Window server, the available check boxes presented in the **Select Component** group are the **Server protect program,** the **Virus pattern,** the **Spyware pattern,** the **Virus Scan Engine,** the **Virus Cleanup Template** and the **Virus Cleanup Engine**. For a 32-bit Windows Server, an **Anti-rootkit Driver** check box, together with the six elements for 64-bit Windows described, is also presented.

3. To apply intended antivirus protections, select the options that correspond to these components in the **Select Component** group. Then, select the options that correspond to the Normal Servers that need to be deployed from the **Select server** tree view. Click **Deploy** to deploy the downloaded elements.

Configuring a Scheduled Deployment

After downloading updates on a scheduled basis, configure a scheduled deployment task to distribute the most recent updates to the Normal Servers.

ServerProtect creates a deploy task by default. See *Default tasks* on page 3-37.

For more information on how to configure a scheduled task, refer to *Creating Tasks* on page 3-38.

Tip: When setting the time for downloading and deploying updates, be sure to set the download time before the deployment.

To configure a scheduled deployment:

1. Do one of the following:

    •   Click **Update** > **Update** on the side bar.

    •   Click **Do** > **Update** from the main menu.

2. Click **Configure** in the **Deploy** section. The **Deploy Option** dialog appears.
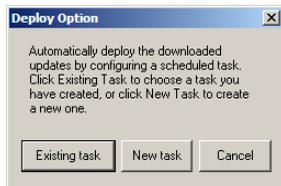
FIGURE 3-47. Deploy Options dialog

3. Do one of the following:

- Click **New task**, to create a task.
- Click **Existing task**, to edit a task.

See *Creating Tasks* on page 3-38 and *Modifying an Existing Task* on page 3-43 for information on how to create or edit a task.

Rolling Back the Previous Deployment Action

ServerProtect can roll back a deployed update action; reverting the system to the previous version of the updated file. Only the virus pattern and the virus scan engine can be rolled back. This is necessary when there is a software compatibility issue or when the update files were corrupted during the original download.

Note: If both the virus pattern and the scan engine files were originally deployed, you can rollback both.

To roll back the previously deployed update:

1. Do one of the following:

- Click **Update** > **Rollback** on the side bar.
- Click **Do** > **Rollback** on the main menu.

The **Rollback** screen appears.
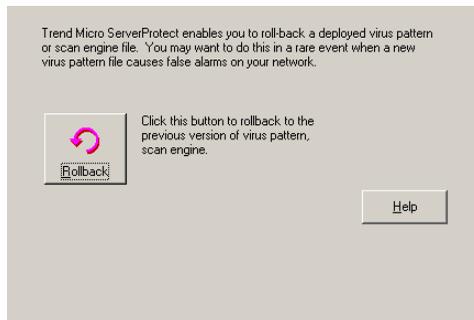
FIGURE 3-48.   Roll Back Configuration dialog

2.   Click **Rollback**. The ServerProtect **Rollback** dialog appears.
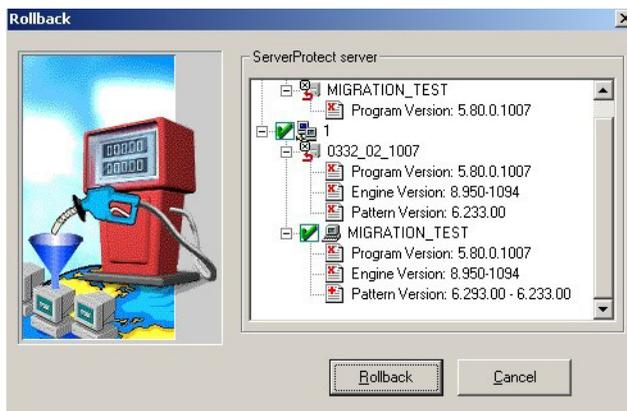
FIGURE 3-49.   Rollback dialog

The screen displays information about the virus pattern file and scan engine that is currently being used by ServerProtect. The respective version and build numbers are also shown.

3.   Select the check boxes of the items you want to roll back, and then click **Rollback**.

> **Note:** You can only roll back the components which is most recently updated, The components can either be a virus pattern or a scan engine.

Managing Tasks

Tasks allow you to schedule Normal Servers to perform multiple functions simultaneously. Using tasks automates routine antivirus maintenance procedures on your network and improves the management of your antivirus policy.

You can define a task to run several procedures at one time in the same manner as macros automate word processing programs, or scripts automate routine network administration tasks.

Tasks are assigned to a "task owner" who is responsible for maintaining the task.

ServerProtect Task Wizard

The ServerProtect Task Wizard provides an intuitive interface for you to easily define a task. You can include the following functions in a task:

- **Real-time Scan setting**: Enables different Real-time Scan options for different tasks, for example, scanning incoming files only when the network performance is normal
- **Scan Now**: Checks whether your server is virus-free
- **Purge logs**: Defines which types of logs to purge from the database. You can enable the automatic purging of virus logs that are older than a preset age.
- **Export logs**: Exports logs as CSV files for use in other applications
- **Print logs**: Chooses a network printer to print logs that meet a certain criteria
- **Run statistics**: Compiles and displays statistics about virus scanning on your server

- **Deploy**: Defines when to distribute the updates of virus pattern and scan engine components to other ServerProtect servers
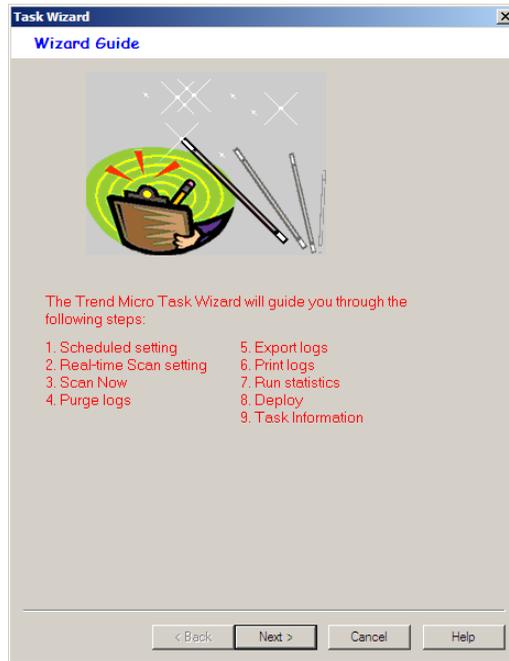
FIGURE 3-50. Task Wizard dialog

Default tasks

Default tasks are created by ServerProtect with every Normal Server installation. When you install ServerProtect for the first time, you immediately have three default tasks: Scan, Statistics, and Deploy. You can edit default tasks, however, you cannot modify the task name or the task owner.

Creating Tasks

New tasks let you set up routine maintenance and configuration procedures.

To create a task:

1. Select the Information Server, domain, or Normal Server on the domain browser tree.

2. Do one of the following:
   - Click **Do** > **Create Task** on the main menu.
   - Click **Task** > **New Task** on the side bar.

3. Click **Create**. The **Create New Task** dialog appears.
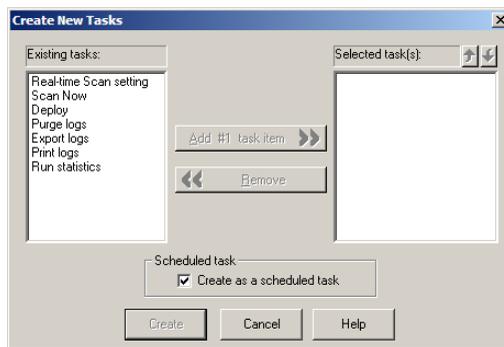
FIGURE 3-51. Create New Tasks dialog

4. Select the functions you want to include in this task in the **Existing tasks** list.

5. Click **Add #n Task Item** to add the selected function to the **Selected task** list. You can continue adding more functions. Alternatively, you can remove a previously selected function.

Tip: You can click the up or down arrow icons next to **Selected task(s)** to change the order in which the functions are performed. The Deploy function should always be the last one on the list.

---

6. Select the **Create as a scheduled task** check box if you want this task to be run according to a specified schedule. You can schedule tasks to run on an hourly basis.

7. Click **Create** to start the wizard and create a task with the selected functions. Click **Cancel** to close the **Create New** dialog without saving your changes.

Creating a Scheduled Task

Creating a scheduled task is easy to configure and save you time.

To create a scheduled task:

1. Follow steps 1 through 6 in the *Creating Tasks* on page 3-38 section. Make sure you select the **Create as a scheduled task** check box under **Scheduled task** (see *Figure 3-51*). The **Task Wizard** dialog appears.

2. Click **Next**. The **Schedule Settings** dialog appears.
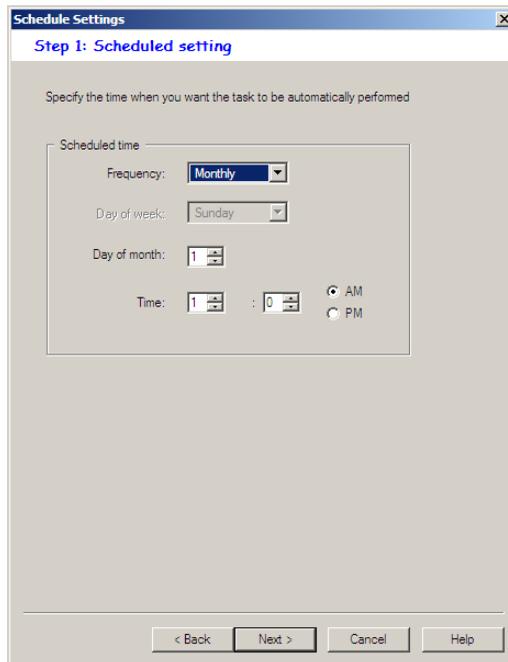
FIGURE 3-52.   Schedule Settings dialog

3. Under **Scheduled time** in the **Frequency** list, click a download frequency. You can select **Monthly**, **Weekly**, **Daily**, **or Hourly**. If you selected **Weekly**, select a day

from the **Day of Week** list. Alternatively, if you selected **Monthly,** click a day in the **Day of month** list.

4. In the **Time** box, type or select the time when you want to update the components, and then click **AM** or **PM**.

5. Click **Next** to proceed with the task wizard configuration.

Specifying a Target for Scan Now

Scan tasks must be run on specific drives. When defining the target drive, you are initially given the option to scan all local drives or specific drives and/or directories. The latter option also allows you to scan another drive on the network.
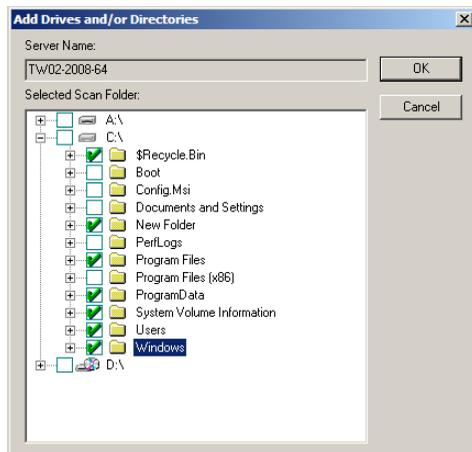
FIGURE 3-53. Add Drives and/or Directories dialog

Creating a Default Task

You can define a default task in the last screen of the task wizard, the **Task Information** dialog, where you define the name and owner of the task. Default tasks affect all Normal Servers managed by an Information Server which means if you add a Normal Server, it will inherit existing default tasks.
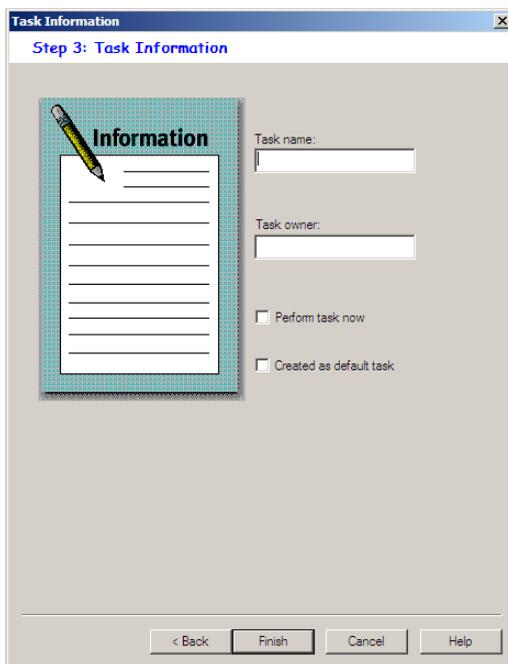
FIGURE 3-54. Task Information dialog

Opening the Existing Task List

The **Existing Task** list displays information about the tasks that have been created. You can use the **Existing Task** list to perform, modify, delete, or view the task definition.

To open the existing task list, do one of the following:

• Click **Task** > **Existing Task** on the side bar.

• Click **Do** > **Existing Task** on the main menu.

The **Existing Task** list is displayed in a table format. The following figure displays the different fields. Note that you can sort the list by clicking on the heading of each field.

FIGURE 3-55. Viewing Existing Tasks table

Note: If the servers to which a task is applied are located in different time zones, the time/date displayed in the **Last Perform Time** and **Next Schedule** fields will reflect the local time for each server.

Running an Existing Task

The **Existing Task** list displays information about all the tasks that have been defined. You can use the **Existing Task** list to perform a task.

To run an existing task:

1. Do one of the following:
    - Click **Task** > **Existing Task** on the side bar.
    - Click **Do** > **Existing Task** on the main menu.

The **Existing Task** list displays all of the tasks that are currently defined within ServerProtect.

2. Select the task that you want to run, and click **Perform Now**.

Modifying an Existing Task

Modifying existing tasks saves you valuable configuration time. This way, you do not need to spend time configuring new tasks.

To modify an existing task:

1. Do one of the following:
   - Click **Task** > **Existing Task** on the side bar.
   - Click **Do** > **Existing Task** on the main menu.

   The **Existing Task** list appears.

2. Click the task in the **Existing Task** list that you want to modify.

3. Click **Modify**. The **Modify Task** dialog appears.
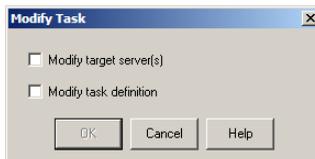
FIGURE 3-56. Modify Task dialog

4. Do one of the following:
   - Select the **Modify target server(s)** check box to change the servers, on which the task is configured to run.
   - Select the **Modify task definition** check box to change the procedures that were used to define the task.

5. Click **OK**.

To modify a target server for an existing task:

1. In the **Select Servers to Apply Tasks** dialog select and add the server on which you want to run the task.

2. Click **Add**.
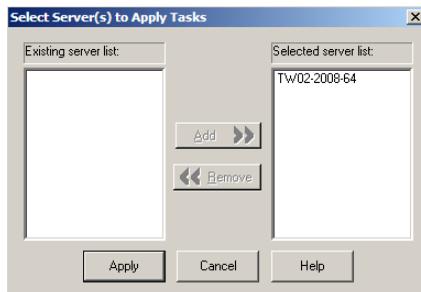
FIGURE 3-57. Select Servers to Apply Tasks dialog

3. Click **Apply**. To close the dialog without saving your changes, click **Cancel**.

To modify a task definition for an existing task:

1. Select each function you want to include in this task in the **Existing Tasks** list.
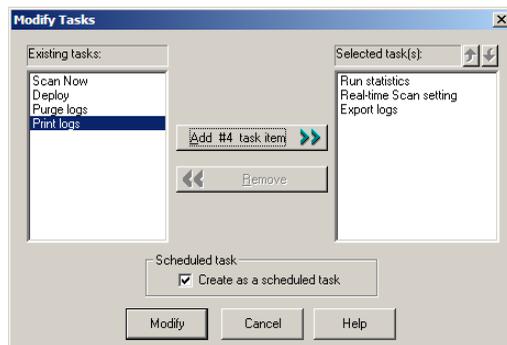
FIGURE 3-58. Modify Tasks dialog

2. Click **Add #n Task Item** to add the function you selected to the **Selected task** list.

If you want this task to be scheduled to run, make sure that you select the **Create as a scheduled task** check box.

Tip: You can click the up or down arrow icons next to **Selected task(s)** to change the order in which the functions are performed. The Deploy function should always be the last one on the list.

---

3. Click **Modify** to start the wizard that will help you create a task with the functions that you have chosen. Click **Cancel** to close the **Create New Task** dialog without saving your changes.

Viewing an Existing Task

The attributes of any existing task can be viewed from the **Existing Task** dialog. This enables you to know exactly what the task will do before executing it.

To view an existing task:

1. Do one of the following:
   - Click **Do** > **Existing Task** on the main menu.
   - Click **Task** > **Existing Task** on the side bar.
2. Select the task in the **Existing Task** list that you want to view.

3. Click **View** at the bottom of the configuration area. Alternatively, you can double-click the task's record entry in the **Existing Task** table. The **View Task Information** dialog appears.
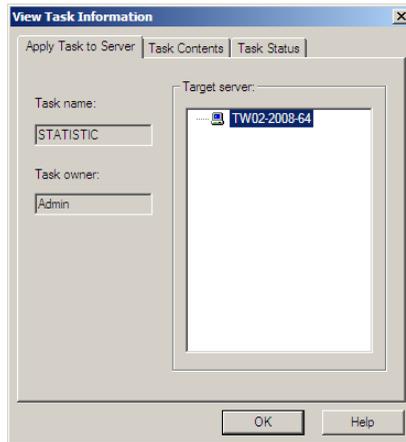
FIGURE 3-59. View Task dialog

This screen contains three tabbed sections labeled **Apply Task to Server**, **Task Contents**, and **Task Status**.

- **Apply Task to Server**: The **Task name** and **Task owner** are displayed on the left side of the tab. The **Target server** displays all the servers on which the task will run on your network.

- **Task Contents**: All of the functions that make up the task are displayed. Select a function in the **Task sequence** list and the function definition will appear in the task definition table on the right.

- **Task Status**: The **Target Server** displays all of the servers on your network on which the task will run. The **Current Status**, **Last Perform Time**, and **Next Schedule** fields display the status of the task and the last time it was run.

4. Click **OK** to close the **View Task Information** dialog.

Removing an Existing Task

The **Existing Task** list displays information about all tasks that have been defined. You can use the **Existing Task** list to delete a task definition.

To remove an existing task:

1. Do one of the following:
   - Click **Do** > **Existing Task** on the main menu.
   - Click **Task** > **Existing Task** on the side bar.
2. In the **Existing Task** list, select the task you want to remove.
3. Click **Remove**.

Configuring Notification Messages

Antivirus software is quite useful if it alerts a user or an administrator when a virus is detected. ServerProtect enables you to configure both notifications and to whom they will be sent.

ServerProtect notifications comprise of standard and outbreak alerts. Alerts can be delivered in various ways. See *Setting Alert Methods* on page 3-52 for all available delivery options.

Standard Alerts

A standard alert is generated whenever a selected event is detected on the designated server. You can append additional text to a notification message.

Notification Events

You can configure ServerProtect to notify you when the following events occur.

- **Virus/Malware detected**: an infected file on the server was detected
- **Spyware/Grayware detected**: spyware or grayware-infected file on the server was detected
- **Attempt to change write-protected file**: detects attempts to change write-protected file settings

- **Real-time configuration change**: detects changes to real-time scan configuration settings
- **Service load/unload**: detects events that stop/start ServerProtect
- **Filer RPC connection success/failure**: Status of an RPC connection to a NetApp Filer
- **Virus pattern out-of-date**: detects whenever the virus pattern file is out-of-date
- **Spyware pattern out-of-date**: detects whenever the Spyware pattern file is out-of-date

To configure a standard alert:

1. Select the Information Server domain, or a Normal Server on the domain browser tree.
2. Do one of the following:
   - Click **Configure** > **Notifications** > **Standard Alert** on the main menu.
   - Click **Set Notification** > **Standard Alert** on the side bar.

The **Standard Alert** screen appears.
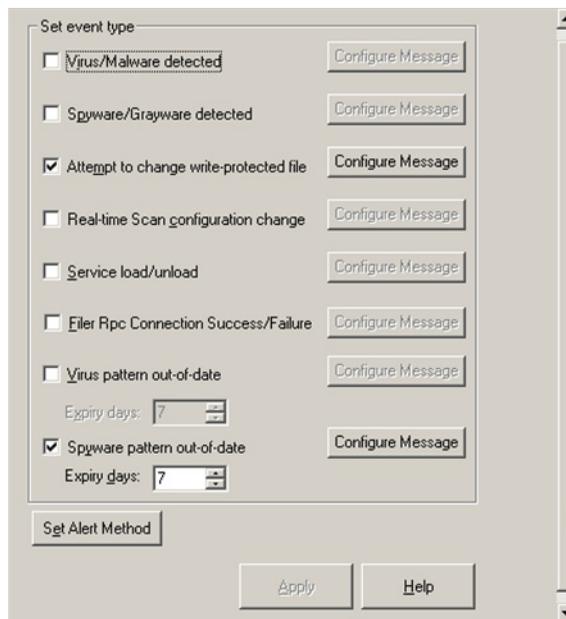
FIGURE 3-60. ServerProtect Standard Alert Configuration Window

3. Select the event type check box(es).

4. Click **Configure Message** for each selected event. The **Configure Alert Message** dialog appears.

5. Type your desired settings, and then click **OK** to close the dialog.

6. Click **Set Alert Method** to select the way that you want to be notified. Refer to *Setting Alert Methods* on page 3-52 for additional information.

Note: To find out more on configuring alert messages, refer to the related topic in the online help.

Outbreak Alerts

Virus outbreaks have a high potential for damage on a corporate network. Whenever the number of virus events exceeds the threshold, an outbreak alert is triggered to notify the system administrator.

This ensures that system administrators or other individuals who need to know about the virus outbreak are notified and can then take action against them. A customized message will be used to alert of an outbreak.

To configure an outbreak alert:

1. Select the Information Server domain, or a Normal Server on the domain browser tree.

2. Do one of the following:

   • Click **Set Notification** > **Outbreak Alert** on the side bar.

   • Click **Configure** > **Notifications** > **Outbreak Alert** on the main menu.

   The **Outbreak Alert** screen appears.

FIGURE 3-61.   ServerProtect Outbreak Alert Events Configuration Window

3. Define the outbreak threshold. Specify the number of viruses to be exceeded, and the period of consideration, in hours, in the boxes provided.

4. Select the notification methods that the alert uses.

5. Click **Configure** to access the notification settings for the selected methods. For additional information about each modification method, refer to *Setting Alert Methods* on page 3-52.

6. Under **Alert Message**, click **Configure Message** to modify the message that will be displayed when there is a virus outbreak.

7. Click **Apply** to save your settings.

Setting Alert Methods

When a virus outbreak occurs, ServerProtect can notify system administrators, and other people you designate using the following methods:

- **Message box**: A standard Windows pop-up message box is displayed on the administrator's computer.
- **Printer**: A document is sent to a local or network printer.
- **Pager**: A message is sent to a pager. This feature requires a modem to be connected to the server that is hosting Trend Micro ServerProtect.
- **Internet Mail**: An email message can be sent according to the user configuration.
- **SNMP Trap**: An alert message is sent to network administrators by SNMP. This integrates with other SNMP-compatible management tools that may be deployed within your company.
- **Windows Event Log**: The detection of the virus is written to the Windows event log.

You can configure one or several notification methods. Instructions to configure email notifications are provided in this document. For other forms of notification, refer to the online help.

To configure an alert to be sent by Internet email:

1. Click either the Information Server domain, or a Normal Server on the domain browser tree.
2. Do one of the following:

    To configure an outbreak alert:

    - Click **Set Notification** > **Outbreak Alert** on the side bar.
    - Click **Configure** > **Notifications** and then **Outbreak Alert** on the main menu.

    To configure a standard alert:

    - Click **Configure** > **Notifications** > **Standard Alert** on the main menu then click **Set Alert Method**.
    - Click **Set Notification** > **Standard Alert** on the side bar and then click **Set Alert Method.**

3. Select the **Internet mail** check box, and then click **Configure**. The **Configure Internet Mail** dialog appears.

FIGURE **3-62.** **Configure Internet Email Alerts dialog**

4. Do the following:

a. Type the name of the mail server in the **Mail Server** text box.

b. Type the subject of the message in the **Subject field** text box.

c. Type the name of the sender in the **From field** text box.

5. Type each recipient of this email message in the **To user(s)** text box and then click **Add**. You can remove a recipient by selecting the user, and then clicking **Remove**.

6. Click **Save & Test** to ensure that the configuration settings are working. If successful, the users that you specified receive a test email message.

7. Click **OK** to save your configuration changes and return to the **Set Alert Method** dialog.

Note: To find out more about configuring alert messages, refer to the related topic in the online help.

Scanning Viruses

ServerProtect provides three scan modes for detecting viruses: Real-time Scan, Scan Now (Manual scan), and Scheduled scan.

Real-time Scan checks all incoming and outgoing files on the server for signs of infection. Scan Now scans on-demand, allowing you to check a server for virus exposure immediately. Scheduled scan checks for infected files on selected ServerProtect servers at predetermined times.

There are five actions for dealing with infected files: Bypass **(**Ignore**)**, Delete, Rename, Quarantine (Move**),** and Clean.

You can do the following:

- Choose the type of files to scan.
- Prevent users from modifying or deleting selected directories/files using the Deny Write list. For more information about configuring the Deny write list, see the related topic in the online help.

Note: The results of each scan are available in the Scan Result logs. You can take action on the infected files directly from the **Scan Result** dialog. This provides a convenient way to take appropriate actions during a virus infection event. For more information, refer to the *Viewing Scan Result Information* topic in the online help.

Defining Actions Against Viruses

ServerProtect lets you configure the kind of action(s) to take against infected files that are found on your network during a Real-time Scan or Scan Now.
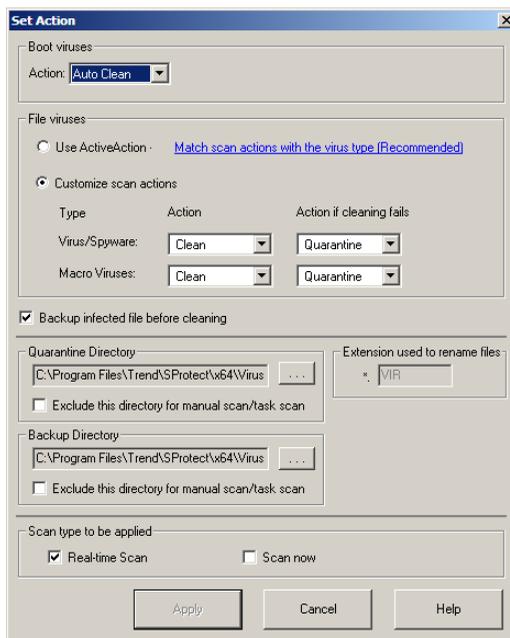
FIGURE **3-63.   Set Virus Action dialog**

To configure virus actions for a virus type:

1. Click **Set Action** from the **Scan Now** or **Real-time Scan** configuration area. The **Set Virus Action** dialog appears.

Note: Spyware doesn't support clean action. If the action of virus is clean/delete, for spyware virus it will only do delete operation.

---

2. Under **Boot Viruses** in the **Action** list**,** click the virus action you want ServerProtect to take when it finds a boot virus. You can select **Auto Clean** or **Bypass**.

3. Under **File Viruses**, do one of the following:

- Click **Use ActiveAction** to set Trend Micro recommended virus actions. Beware that the action can be taken to handle spyware infection is limited to **Bypass**, and that the action **Clean** is not supported to handle spyware infection. Applying the **Clean** action to a spyware infected file will delete the file.

   Note: When using ActiveAction, spyware action will be bypass/bypass.

- Click **Customize scan actions**, to select the appropriate action to take against the file and macro viruses in the **Action** and **Action if cleaning fails** lists. See *When ServerProtect Finds a Virus (Virus Actions)* on page 1-13. For more information about ActiveAction, see *IntelliScan* on page 1-20.

   Note: If you selected a **Clean** action, we recommend that you select the **Backup infected file before cleaning** check box. The virus cleaning process can, on rare occasions, damage files and make them unusable.

You should exclude both the backup and quarantine directories from scanning. Refer to the *Directory Exclusion List* topic in the online help for more information. The selected scan type is displayed under **Scan type to be applied**.

4. Click **Apply** to start using these settings.

Scanning Profiles

Real-time Scan and Scan Now configurations can be saved as scanning profiles that can then be used to create or modify tasks. Alternatively, you can delete profiles if they are no longer needed. Scanning profiles can be applied when configuring Scan Now and Real-time Scan tasks. For more information, see *Choosing a scan profile* in the online help.

For scheduled scans, that is, scheduled scan tasks, you can either choose an existing scanning profile or create your own. See *Modifying an Existing Task* on page 3-43.

To save a scanning profile:

1. Configure a Real-time Scan or Scan Now. See *Configuring Scan* on page 3-58 and *Configuring Scan Now* on page 3-61.

2. Click **Save As/ Delete Profile**. The **Save/Delete Profile** dialog appears.
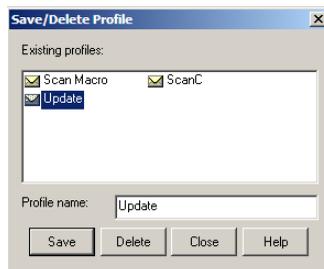
FIGURE 3-64. Save/Delete Profile dialog

3. Type a profile name in the **Profile name** field.

4. Click **Save** to save the new profile. Alternatively, click **Close** to close the dialog without saving it.

To delete a scanning profile:

1. Do one of the following:

   - Click **Scan Now** > **Scan Now** on the side bar.

   - Click **Do** > **Scan Now** on the main menu.

   - Click **Set Scan option** > **Real-time Scan** on the side bar.

2. Click **Save As/ Delete Profile**. The **Save/Delete Profile** dialog appears.

3. Click the profile you want to delete in the **Existing Profiles** list.

4. Click **Delete** to delete the profile. Alternatively, click **Close** to close the dialog without deleting it.

Using Real-Time Scan

Real-time Scan constantly scans all files that are accessed and provides powerful virus protection that runs in the background. The default setting for the ServerProtect Real-time Scan function is *Incoming & outgoing*. This means that all incoming/outgoing files are monitored, thus infected files are prevented from being copied to or from a server.

Configuring Scan

The following scan options are specific to Real-time Scan:

- **Scan floppy at startup**: Your floppy disk drive is scanned for boot viruses when you turn your computer on. Any diskette inside your floppy disk drive is also scanned. This prevents you from booting your computer with an infected diskette.

- **Scan floppy at shutdown**: Your computer's floppy disk drive is checked for boot viruses when the computer is shut down and any diskette inside it is also scanned.

- **Scan floppy boot area**: This option scans the floppy boot area of your computer. This feature protects against Master Boot Record viruses.

- **MacroTrap**: ServerProtect includes patented MacroTrap™ technology to guard against macro viruses in Microsoft™ Office files and templates.

- **Scan OLE layers**: This option scans embedded files. OLE layer scan offers five layers of protection. See *OLE Layer Scan* on page 1-20 for more information.

- **Scan mapped network drive**: This option scans any mapped network drive. You should have an existing network mapped drive for this option to work.

To configure Real-time Scan:

1. Select the Information Server, domain, or a Normal Server on the domain browser tree.

2. Do one of the following:
   - Click **Set Scan Option** > **Real-time Scan** on the side bar.

- Click **Configure** > **Scan Options** > **Real time Scan** on the main menu.
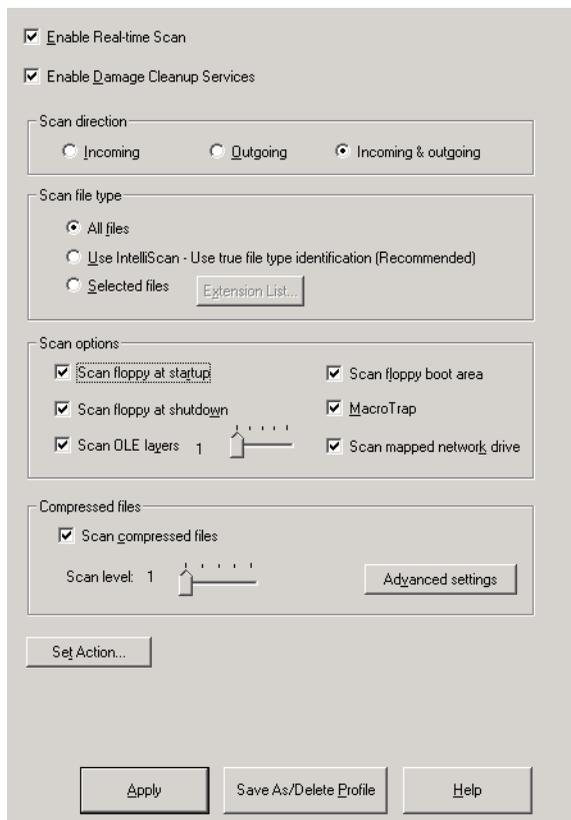
FIGURE 3-65.   Real-time Scanning Configuration Window

3. Select the **Enable real-time scan** check box.

4. Set the **Enable Damage Cleanup Services** check box so that the Virus Cleanup engine scans for and removes Trojans and Trojan processes. It supports 32-bit and 64-bit platforms. Clear the check box to disable the service.

5. Under **Scan direction** choose one of the following:

   - **Incoming**: Scans files copied to the server

- • **Outgoing**: Scans files being copied from the server
- • **Incoming and Outgoing**: Scans all incoming and outgoing files on the server

6. Under **Scan file type,** choose one of the following:

- • **All files:** Scans all file types
- • **IntelliScan**: Scans files using true file type identification

    See *IntelliScan* on page 1-20.

- • **Selected files**: Scans only specified files

    If you choose **Selected files,** click **Extension List** to define the file types that you want to scan. Refer to *Selecting File Types to Scan* on page 3-66.

7. Under **Scan options**, select one or more from the following check boxes:

- • Scan floppy at start up
- • Scan floppy at shutdown
- • Scan OLE layers
- • Scan floppy boot area
- • MacroTrap
- • Scan mapped network drive

    See *Configuring Scan* on page 3-58 for additional information on each scan option.

8. Select the **Scan compressed files** check box to scan compressed files and then move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the *Compressed file scan* topic in the online help.

Note: If you choose to scan selected file types in step 5, make sure you select the extensions of compressed files in the extension list.

---

9. Click **Set Action** to configure how ServerProtect acts on infected files. See *Defining Actions Against Viruses* on page 3-55.

10. Click **Apply** to save your changes or click **Save As Profile** to recall your configuration settings at a later time.

Using Scan Now (Manual Scan)

Scan Now performs a scan on demand. Use Scan Now if you suspect a server has been infected.

Configuring Scan Now

You can configure the following for Scan Now:

- Scan target
- Scan file type
- Scan options
- Compressed file scanning
- Scan priority
- Scan action

To configure Scan Now:

1. Click the Information Server, domain, or a Normal Server on the domain browser tree.

2. Do one of the following to bring about the configuration pane for Scan Now operation, as shown in Figure 3-31:

    - Click **Scan Now** > **Scan Now** on the side bar.

- Click **Do** > **Scan Now** on the main menu.

FIGURE 3-66. Scan Now Configuration dialog

3. Set **Enable Damage Cleanup Service** check box to enable the service. Clear it to disable the service.

4. Under **Scan target**, choose one of the following:

- **All local drives**: Scans all drives in a server
- **Selected drives/directories**: Scans specific drives or directories on a server

Click **Browse.** The **Add Drives and/or Directories** dialog appears. Select the check box(es) for the drives or directories you want to scan, then click **OK** to close the dialog.
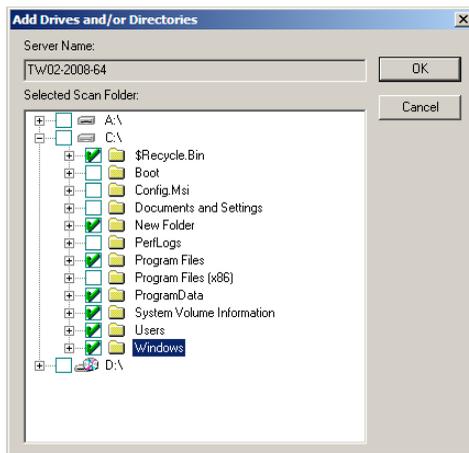
FIGURE **3-67. Add Drives and/or Directories dialog**

5. Under **Scan file type**, choose one of the following:

    • **All files**: Scans all files

    • **Use IntelliScan**: Scans files using true file type identification

       See *IntelliScan* on page 1-20.

    • **Selected files**: Scans only specified files

       Click **Extension List** to define the file types that you want to scan. Refer to *Selecting File Types to Scan* on page 3-66.

6. Under **Scan options**, select **Scan OLE layers**. Move the **Scan OLE layers** slider to set the number of OLE layers. ServerProtect can scan up to five layers.

7. Under **Compressed file scanning**, select the **Scan compressed files** check box. Move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the *Compressed file scan* topic in the online help.

Note: If you choose to scan selected file types in step 4, make sure you include the extensions of compressed files in the extension list.

---

8. Under **Scan priority**, click **Low, Middle**, or **High**. A high scan priority consumes more CPU resources, but can complete scan jobs faster.

9. Click **Set Action** to configure how ServerProtect acts on infected files. See *Defining Actions Against Viruses* on page 3-55.

10. Click **Apply** to save the changes or click **Save As Profile** to recall the configuration settings at a later time.

Running the Scan Now Tool on Windows Normal Servers

Use the Scan Now tool to scan servers of Microsoft Windows Server family without accessing the Management Console. Scan Now performs the scan according to the Scan Now configurations you have set in the Management Console (for example, Scan target, Scan file type).

To run the Scan Now tool:

1. Click **Start** > **Programs** > **Accessories** > **Windows Explorer** on the Normal Server. The **Windows Explorer** dialog appears.

2. Click the folder where you installed ServerProtect. The default location for a 32-bit operating system is:

   `C:\Program Files\Trend\SProtect`

   The default location for a 64-bit operating system is:

   `C:\Program Files\Trend\SProtect\x64`

3. Double-click **ScanNow.EXE**. A Scan Now is performed.

To stop Scan Now:

1. Click **Start > Run** on the Normal Server. The **Run** dialog appears.

2. Click **Browse** and locate the ScanNow.EXE file.

   The default location for a 32-bit operating system is:

   `C:\Program Files\Trend\SProtect`

   The default location for a 64-bit operating system is:

```
C:\Program Files\Trend\SProtect\x64
```

3. Run the tool with the "stop" switch as shown below:

   For a 32-bit operating system:

   ```
   C:\Program Files\Trend\SProtect\ScanNow.exe /STOP
   ```

   For a 64-bit operating system:

   ```
   C:\Program Files\Trend\SProtect\x64\ScanNow.exe /STOP
   ```

4. Click **OK**. Scan Now stops.

Note: You must include a space between the file name and the Stop switch.

Scheduled Scanning

A scheduled scan scans files at the time and frequency configured. Use scheduled scans to automate routine scans on your Normal Servers. You can create a scheduled Scan Now or Real-time Scan by using a scheduled task.

Configuring a Scheduled Scan

You can configure a scheduled Scan Now or Real-time Scan by using a scheduled task. Refer to *Creating Tasks* on page 3-38 for more information.

Note: When a ServerProtect server is installed, ServerProtect automatically applies a Scan task to the server. The default Scan task is set to scan all your local directories every Friday.

If the existing task does not suit your needs, you can either edit the default task, or create a new one. The ServerProtect Task Wizard guides you through the process of creating new tasks.

Selecting File Types to Scan

While configuring a Real-time Scan, Scan Now, or scheduled scan (task scan), ServerProtect lets you choose what kinds of files to scan by choosing the file extensions. Since only certain kinds of files can contain viruses, you can benefit from this function by only scanning those file types that are more likely to be infected.

To include a file extension for scanning:

1. In the Real-time Scan or Scan Now configuration area, under **Scan file type**, click **Selected files**, and then click **Extension List** to define the file types you want to scan. The **Select File for scanning** dialog then appears.
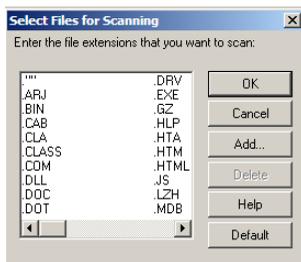
FIGURE 3-68.   Select Files for Scanning dialog

2. Do one of the following:

    *   Click **Add**. The **Add Program File Extension** dialog appears.

FIGURE 3-69.   Add Program File Extension dialog

    Type the file extension that you want to **include** for scanning and click **OK**. Alternatively, click **Cancel** to close the dialog without saving your changes.

    *   Click **Default** to add all the default file extensions and then click **OK**. Any customized extensions will be lost.

The default setting provides sufficient protection for most environments. The following are the default file extensions:

.ARJ	.BIN	.CAB	.CLA
.CLASS	.COM	.DLL	.DOC
.DOT	.DRV	.EXE	.GZ
.HLP	.HTA	.HTM	.HTML
.JS	.LZH	.MDB	.MPP
.MPT	.MSG	.OCX	.OFT
.OVL	.PIF	.POT	.PPS
.PPT	.RAR	.RTF	.SCR
.SHS	.SYS	.TAR	.VBS
.VSD	.VST	.XLA	.XLS
.XLT	.Z	.ZIP	

- Select the file extension you want to delete, and then click **Delete**.

To exclude a file extension from scanning:

1. Select **Set Scan Option > Exclusion List** from the left side bar.

2. Click **Configure > Scan Options > Exclusion List** on the main menu.

3. Under **Excluded file extension list**, click **Add**. The **Add Program File Extension** dialog box appears.
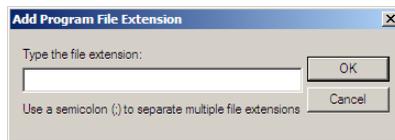
FIGURE 3-70. Add Program File Extension dialog

4. Type the file extensions that you want to **exclude** from being scanned. You can add multiple file extension separated by a semicolon (;).

5. Click **OK**.

6. To delete a previously typed file extension, select the file name from the **Excluded file extension list**, and then click **Remove**.

7. Click **Apply**.

Chapter 4

Upgrade and Troubleshoot ServerProtect for NetApp

ServerProtect supports the product upgrading and migration from the previous versions of the product. The configuration settings of older versions can be migrated and stay effective in the new version of application

The version 5.8 installation program can detect the existence of ServerProtect components, including the Normal Server, the Information Server and Management Console. The upgrading and migration feature is an integral part of the ServerProtect installation program. This chapter introduces the key concepts and presents to the user how to use this feature. This chapter also introduces the troubleshooting for ServerProtect for NetApp.

The topics included in this chapter are:

Upgrading Existing ServerProtect

Many users of the ServerProtect have a previous version of product already installed on their network server system, such as ServerProtect 5.62. The upgrade feature integrated in ServerProtect 5.8 offers a number of upgrade options for the users to choose, whichever the most effective will be to serve the purpose. This overview explains each of the options and introduces the related key concepts.

1. Because ServerProtect 5.8 Information Server refuses adding and moving Normal Server request to old normal Servers (version of 5.62), make sure that you move all the old Normal Servers need upgrade into the Information Server to be upgraded.

Note: You cannot add an existing normal server by selecting "Add a Normal Server" or "Move a Normal Server".

---

2. Launch the ServerProtect installation and make proper selection to install an Information Server of the latest version of ServerProtect 5.8. To upgrade an existing Information Server, simply select the same target server during the course of installation.See *Use the Installation Package to Upgrade ServerProtect Locally* on page 4-3 for details.

3. The next move is to install the Management Console component if the latest version one is not yet in place. See *Use the Installation Package to Upgrade ServerProtect Locally* on page 4-3 for detailed information.

4. At this point the Management Console and the Information Server are ready. The Normal Server can be upgraded by the following methods:

• Use the installation package to perform the upgrade locally.

• Use the installation package to perform the upgrade remotely across the network.

• Use silent mode installation to perform the upgrade. The silent mode installation should be used to upgrade the machine only with Normal Server installed. if the silent installer detects that other components is installed, it will terminate and does nothing. We recommend that this method be the only one to upgrade the Normal Servers. It can prevent upgrading Information Server on the remote target machine by accident.

• Use Deploy program feature of ServerProtect 5.8 to perform the upgrade.

The rest of this chapter will focus on presenting comprehensive information. While the major attention is to describe how to perform Normal Server upgrading, the upgrade details for other components, together with related key concepts, will also be presented in aiding the users to achieve an effective and smooth program upgrade.

Use the Installation Package to Upgrade ServerProtect Locally

Because the Upgrade feature is an integral part of the ServerProtect installation program, no differences exist at all in term of user interface appearances and program behaviors. Upgrading the ServerProtect locally is by far the most straight-forward and reliable option. It is also the only way to install or upgrade a Management Console component.

To initiate a local upgrade session, use the installation package to launch the installation session in the local computer. See *Installing ServerProtect* on page 2-9 for detailed information. The installation program will the user through the whole procedure. At the **ServerProtect** Select Component dialog as shown in the following:
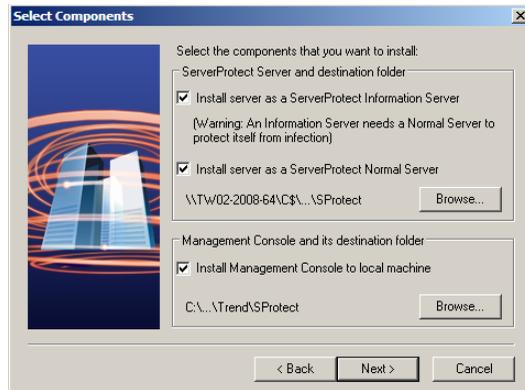
FIGURE 4-71.   The ServerProtect Select Component Window

> **Note:** Always keep in mind that all those components known to be existing in the system must be selected to achieve a successful upgrade.

Set the check box corresponding to those options need to be upgraded and click **Browse...** to bring up **ServerProtect Installation Path Selection** dialog. See *ServerProtect Install Path Selection screen* on page 2-17. Navigate to the target folder which needs to be upgraded on the local computer. The installation program will complete the upgrade after copying the program files and starting all related services.

> **Note:** When make the selection to upgrade one ServerProtect component, keep in mind to select all the existing components, including those of the latest version already. Otherwise the installation program will pop up message box, stating that other components must be choose to continue, and bring the user back to the **ServerProtect Selection Component** dialog and request the user to redo the selection

> **Note:** If Trend Micro Control Manager Agent is installed, it should be upgraded after the Information Server is installed.

Use the Installation Package to Upgrade ServerProtect Remotely

The way to remotely upgrade the ServerProtect is not very different to that of doing it locally. After launching the ServerProtect installation program, accepting the agreement terms and submitting the correct serial number, the ServerProtect Select Component screen appears. When choosing a Normal Servers as the upgrade candidate using **Browser...** button to locate the target server, instead of exploring in the local computer, the user can navigate to the connected server network system, locate the Normal Server or Information Server need to be upgraded and perform the upgrade operation just as doing it locally. See *Installing ServerProtect* on page 2-9 for detailed information.

> **Note:** ServerProtect does not support installing or upgrading the Management Console component remotely.

Perform a Silent Mode Installation to Upgrade the Normal Servers

It is well known that, under Microsoft Windows environment, executing program by running it in DOS command line window has certain advantages. The Windows shell is capable of interpreting commands which compose a script file. One can compose such a file to automate certain tasks. In ServerProtect 5.8, capable of launching the installation program in silent mode let the users to enjoy such advantages.

Note: The silent install should be used to upgrade the server only with normal server exists. When silent installer detects the other components, it will quit and do nothing.

To install ServerProtect in silent mode:

1. Install an Information Server.

2. Locate the **SMS** folder in the default installation path, and share it. Make sure the target servers you want to install as Normal Servers can access the folder. If you want to perform more than one silent installation, map the **SMS** folder on the target servers.

3. At the target server, open a command prompt, go to the **SMS** folder or drive that is mapped to the folder, and then enter the following command:

```
<drive>:\setup -SMS -s -m"SPNAF"
```

Example:

a. At the target server, map the SMS folder to drive "M".

b. Open a command prompt.

c. For example, to go to drive **M**, type the following:

```
M:\setup -SMS -s -m"SPNAF"
```

d. Press **Enter**.

Silent install will proceed and the target server will be registered with the Information Server.

For a silent installation, Normal Servers are installed in the "SMS" domain. There is no way to change the domain name during the silent installation. You can, however, rename the SMS domain after all the Normal Servers have been installed.

You can also specify a path to which ServerProtect is installed. For example, to install ServerProtect to the path "`D:\Utility\AntiVirus\SProtect`" do the following:

1. Locate the `Setup.ini` file in the source folder.

2. Add the following lines:

   `[CommonSection]`

   `ServerTargetUNCPath=D$\Utility\AntiVirus\SProtect`

   Where:

   ServerTargetUNCPath: Sets the location where the Normal Server is installed.

To license the installed Normal Server, add the following lines to the `Setup.ini` file in the source folder.

   `[CommonSection]`

   `ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX`

   Where:

   XXXX-XXXX-XXXX-XXXX-XXXX: Represents the legal serial number.

You may not be able to register a Normal Server under the "SMS" domain due to the use of a domain controller on the Information Server. To resolve this issue, configure an IP address before using silent install.

To configure an IP address, do the following:

1. Go to the `Setup.ini` file in the SMS folder.

2. Replace the host name with its IP address next to **AgentName** then save the file.

Note: During the course of perform upgrade in silent mode, caution should be excised when sharing with others the SMS folder so that all those target servers needs to be upgraded are included. See *Installing ServerProtect in Silent Mode* on page 2-32 for detailed information to use this powerful tool.

Use the Deploy Program to Upgrade the Normal Servers

Performing upgrade using the Deploy feature is the most convenient way to upgrade the obsolete Normal Servers in a server network system. The new Normal Server program code, with the rest of antivirus elements such as spyware and virus pattern files, scan

engine and DCE services, will be downloaded to one of the Information Server and deployed into the system. The only action for a server network administrator to take is choosing in the program's UI element to do so.

Note: When deploy program, all Information Server's and Management Console's files are copied into the Normal Server. This operation will not create Information Server service and Management Console application.

To use ServerProtect 5.8 upgrade:

1. If the Information Server is connected to the Trend Micro Control Manager Server, download the following:

   • From the main console, click **Update > Update** or click **Do > Update** from the main menu.

   • Click **Configure** to open the **Download Option** screen.

   • Change the **Download source** to **Internet**, and change the download URL to:

   http://spnaf58-p.activeupdate.trendmicro.com/activeupdat e

   • Click **OK** to apply the settings.

   • Click **Download Now**.

   • After the download completes, verify that *server.ini* located in: {ServerProtect home directory}\SpntShare\ contains the following information:

Note: The ServerProtect Information Server default path is: C:\Program Files\Trend\Sprotect\SpntShare.

[Info_186_50000_1_5121]

Version=5.8

Update_Path=serverprotect/spnt580/auspnt50.zip, 43914

Min=5.0

Max=6.0

Path=ServerProtect/SPNT58.zip, 36730864

[Info_2_50000_1_1]

Version=5.8

Update_Path=serverprotect/spnt580/auspnt50.zip, 43914

Min=5.0

Max=6.0

Path=ServerProtect/SPNT58.zip, 39824843

2. Do one of the following:

   • Click **Update** > **Update** on the side bar.

   • Click **Do** > **Update** from the main menu.

3. Click **Deploy Now**. A confirmation dialog appears. Click **Yes** to proceed with the manual update deployment. The **Deploy** dialog appears.
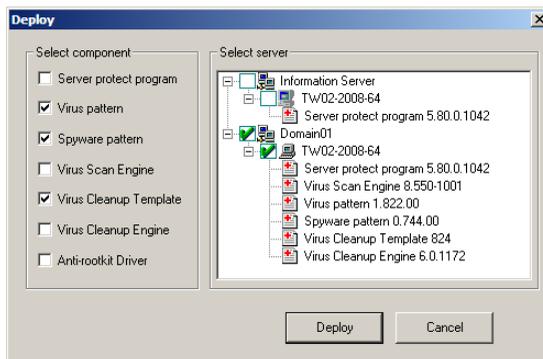
FIGURE 4-72. The Deploy Window

4. To enable upgrading Normal Server feature by download and deployment, simply set the check box corresponding to the item **ServerProtect Program.** Note that this option is not among the three antivirus components selected as default at application initialization. Click **Deploy** to dismiss the Deploy dialog and conclude the upgrade operation.

Upgrading ServerProtect for NetApp

If you are currently using an older version of ServerProtect for NetApp, you can upgrade to this new version. The procedure for upgrading ServerProtect for NetApp is the same as for ServerProtect for Windows.

Note: After upgrading to this version of ServerProtect for NetApp, all configuration options from your previous ServerProtect for NetApp installation will remain the same.

To upgrade from previous versions of ServerProtect for NetApp, do the following:

1.   Verify the system requirements for this new version.
2.   See *Upgrading Existing ServerProtect* on page 4-2

Upgrading the ServerProtect Evaluation Copy

To enjoy the benefits of automatic software updates and technical support, upgrade to a registered version of ServerProtect for NetApp. Refer to the appendix for detailed instructions on how to upgrade your evaluation copy to the full version of ServerProtect.

Troubleshooting ServerProtect for NetApp

This section contains troubleshooting information and may assist you in finding a solution to frequently asked questions.

NetApp Filers do not recognize ServerProtect for NetApp Scan Servers

Description:

After a power cycle on the NetApp Filer, the ServerProtect for NetApp Scan Server returns event 213, which is described as follows:

Cannot add a connection to Filer. The network path was not found. Running the "vscan scanners" command on the NetApp filer returns the following message:

```
"No virus scanners are registered with the filer."
```

The ServerProtect for NetApp Scan Servers still manage to obtain pattern updates from Trend update servers.

Solution:

Confirm the following conditions exist:

- Remote Procedure Call (RPC) is enabled on the servers
- Vscan is turned "On" on the NetApp Filer
- The Common Internet File System (CIFS) default share (C$) still exists

After confirming these conditions, do the following:

1. 1. Right-click a Scan Server, and then select **Filer List** on the domain browser tree. The **Filer List** screen appears.
2. Select one or more NetApp Filers from the list. To multi-select several NetApp Filers, press the CTRL key as you select.
3. Click **Logon Info**. The **Logon Information** screen appears.
4. Verify the information is correct. Otherwise, reenter it.
5. Click **OK**.

After completing these steps, repeat the registration of the Scan Server in the NetApp Filer. If the password for the administrator account was recently changed, the changes may not take effect until a start up/power-cycle of the NetApp Filer occurs.

The Scan Server completed scan on a file but original request was not found when scanning large files on the NetApp Filer

Description:

When scanning large files on the Filer in ServerProtect for NetApp, the following message appears:

```
"[Server] completed scan on [FileName] but original
request was not found."
```

Solution:

This situation occurs because the scan period encountered a time out due to the large size of the file. Resolve this issue by extending the Time Out period between the Filer and the Scan Server.

To extend the Time Out period between the Filer and the Scan Server, perform the following steps on the Scan Server:

1. Run Regedit.

2. Browse to the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\Current
   Version\Engine\Filers
   ```

3. Set the Value Data to the desired TimeOut period in the **ScanFilerTimeOut** DWORD.

The unit of ScanFilerTimeOut is in seconds; this is the timeout value for the Scan Server to scan a file.

Note: Default timeout period for ServerProtect is 24 seconds.

To disable this warning, add the **ScanTimeOutLog** DWORD Value to the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\CurrentVer
sion\Engine\Filers
```

Possible values for ScanTimeOutLog:

1 - Enable logging of files not scanned due to time out

0 - Disable logging of files not scanned due to time out

Configuring the ServerProtect for NetApp to scan all file types

Description:

How to configure ServerProtect for NetApp to scan all file types?

Solution:

To scan all files placed on the NetApp Filer, change the extension table of the NetApp Filer so it supports all file extensions.

To make sure the extension table of the NetApp Filer supports all file extensions, type the following at the NetApp Filer command prompt:

```
filer> vscan extensions add ???
```

Note: The above command will make the filer scan all file types regardless of their extension. The NetApp Filer wild card is a question mark (?) and not an asterisk (*).

To add any file extension into the NetApp Filer's extension table, type the following at the NetApp Filer command prompt:

```
filer> vscan extensions add vbs
```

The above command will make the NetApp Filer scan file with a ".VBS" extension. You can replace vbs with any three-letter file extension.

Scanning all files can degrade the NetApp Filer's performance and slow down virus scanning. It is recommended to scan files that are prone to viruses.

Chapter 5

Managing ServerProtect with Trend Micro Control Manager™

Trend Micro Control Manager (TMCM) delivers powerful centralized management of antivirus and content security solutions deployed throughout the network. With single point-of-contact administration, monitoring, and deployment, corporations can more effectively manage their antivirus and content security strategies enterprise-wide.

Because it is Web-based, Control Manager can be accessed from any server that runs Microsoft™ Internet Explorer. Unlike the Management Console, The Control Manager Web-console allows you to manage several Information Servers at the same time giving you greater control and flexibility over your antivirus strategy.

A ServerProtect Information Server can only manage the Normal Servers that are registered with it. Control Manager, on the other hand, can control groups of Information Servers, and consequently the Normal Servers they manage. Thereby simplifying the management of large networks.

The topics included in this chapter are:

- *What is Trend Micro Control Manager?* on page 5-2
- *Installing and Removing Control Manager Agent for ServerProtect* on page 5-3
- *Control Manager Agent for ServerProtect Features* on page 5-6

What is Trend Micro Control Manager?

Control Manager is a software management solution that gives an administrator the ability to control antivirus and content security programs from a central location -- regardless of the program's physical location or platform. This application simplifies the administration of a corporate virus and content security policy.

Control Manager provides a comprehensive view of the entire network, identifying how Trend Micro products and services, including ServerProtect, can be deployed to create effective, targeted antivirus strategies.

Control Manager maintains a connection with the update server, which provides knowledge and services developed by TrendLabs™. This process enables administrators to stay abreast of the latest virus activity and to be proactive in responding to potential threats in their own environment.

During an attack, the Trend Micro Control Manager Web-based console functions as a centralized "command post" to monitor the outbreak progress, implement containment strategies, deploy newly downloaded pattern files as soon as they become available, and manage cleanup activities. The degree of containment affects all kinds of costs from the effects of the virus on employee productivity to the amount of time needed for cleanup.

Control Manager is key component of the Trend Micro Enterprise Protection Strategy. Trend Micro Enterprise Protection Strategy (TM EPS) delivers a framework for coordinated enterprise protection of the virus outbreak life cycle.

The virus outbreak lifestyle is comprised of three primary phases: outbreak prevention, pattern file generation and deployment, and damage assessment and cleanup. Designed to meet enterprise demands for comprehensive antivirus protection, TM EPS offers a flexible architecture composed of scalable, multi-platform services, products, centralized management and knowledge.

TM EPS transforms the traditional point-based approach to antivirus protection into an enterprise-wide security strategy through centralized deployment of outbreak prevention, detection, protection, and cleanup strategies across the network.

Control Manager offers you the following benefits:

• Proactive outbreak prevention

• Secure communication infrastructure

• Task delegation

- Command tracking

- Real-time product control

- Centralized installation of agents

- Centralized update control

- Centralized configuration

- Centralized log reporting

Installing and Removing Control Manager Agent for ServerProtect

Installing the CM agent for ServerProtect is a two-step process:

1. Obtaining the public encryption key from the Control Manager server.

2. Installing the agent on Information Servers.

You need the following information before deploying the agents:

- Fully Qualified Domain Names (FQDN) or IP addresses of the Control Manager server

- Presence of shared drives on the target ServerProtect Information Server. There must be at least one shared drive on the target server to install an agent.

- A User ID that has privileges to administer the Control Manager server

- The location of the Control Manager public encryption key you intend to use to register the agents

Obtaining the Public Key

The first step in the Control Manager agent installation process is obtaining the public encryption key.

To obtain the public encryption key needed for installation:

1. Open the Control Manager console at:

   ```
   https://computer name/webapp/login.aspx
   ```

Where computer name is the IP address or host name of the Control Manager server. The Control Manager console appears.

2. Type a user name and password in the **Username** and **Password** field. The user name must have access privileges for the Control Manager console and can be an Operator, Power User, or Administrator.

3. Click **Administration** on the menu.

4. Click **Add/Remove Product Agents** on the left menu.

5. Right-click the **public encryption key** link, then select **Save Target As**. Save the public encryption key in a location that is accessible to the server on which the agent will be installed.

Installing the Agent

The second step is installing Control Manager agents on all ServerProtect Information Servers.

To install the agent:

1. Log on to the Information Server using a Windows Administrator account with Domain Administrator privileges.

2. Double-click Setup.exe under the CMAgent folder in the ServerProtect CD-ROM to start the installation process. The **Trend Micro Control Manager Agent for ServerProtect** setup screen appears.

3. On the **Welcome** screen, click **Next**. Read the license agreement; you must agree to the license conditions to proceed with Setup. Click **Next**, the **Setup Control Manager Agent** screen appears.

4. Type an administrator account in **User ID**. Be sure to maintain this account. If the account used here is deleted, either deliberately or accidentally, you are no longer able to manage the agent.

Note: The User ID should be previously created with administrator privileges in the Control Manager server.

---

5. When the **Message Routing Path** screen appears, set the path for incoming and outgoing messages. Outgoing messages can be sent either directly or via a proxy

server. Click either one, and then click **Next**. The **Register with Control Manager Agent** screen appears.

Incoming messages can be received using any of the following methods:

- **Any host**: Accept message from any source
- **IP Port forwarding**: Type the IP address and port number that have been mapped for Control Manager communication
- **Proxy server**: Select the **Proxy Server Communication** check box to specify the proxy server IP address, port number, and type (HTTP or SOCKS 4). If your proxy server requires authentication, select the **Authentication required** check box and in **User name** and **Password**, specify the correct user name and password.

6. Click **Import** to set up secure communications with the Control Manager server. Locate the public encryption key, E2EPublic.dat, of the Control Manager server you are registering the agent with.

7. Follow the installation on-screen instructions to complete the installation.

Removing the Agent

The Control Manager agent can be easily removed from ServerProtect Information Server computer.

To remove the Trend Micro Control Manager Agent for ServerProtect:

1. On an Information Server computer, click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

2. Click **Trend Micro Control Manager Agent for ServerProtect**, and then click **Remove**. A message box appears.

3. Click **Yes** to remove the Control Manager Agent for ServerProtect.

4. Click **Close** to finish.

Control Manager Agent for ServerProtect Features

Control Manager agent for ServerProtect includes several features to manage ServerProtect.

Note: Only some of the ServerProtect Management Console features are available in the Control Manager Web-console.

Centralized Configuration

Centralized configuration, using the Product Directory and cascading management structure, allows you to coordinate virus-response and content security efforts from a single management console. This ensures consistent enforcement of your organization's virus and content security policies.

Proactive Outbreak Prevention

Outbreak Prevention Services (OPS) is a Trend Micro service you can access using Control Manager to take proactive steps against new virus threats before the necessary virus pattern files are available. By bridging the gap between threat notification and virus pattern delivery, enterprises can quickly control viral outbreaks, minimize system damage, and prevent undue downtime.

OPS is a key component of the Trend Micro Enterprise Protection Strategy™ (EPS) This component provides security measures to defend your network against new generation threats, such as CodeRed and Nimda.

Note: Additional EPS information can be found on the Trend Micro Web site at www.trendmicro.com.

OPS provides:

- Timely notification of new threats
- Continuous and comprehensive updates on the status of the outbreak
- Threat specific recommendations on how to contain viruses
- Prompt delivery of virus-specific product settings called "policies"

Secure Communication Infrastructure

The Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages with or without authentication.

Secure Configuration and Component Download

The secure configuration feature allows you to configure security levels to access the Management Console. The component download feature enables you to download these components:

- Virus pattern
- Scan engine

Task Delegation

System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do to the Control Manager network. You can track account usage using the user logs.

Command Tracking

The command tracking feature allows you to monitor all commands executed using the Control Manager management console. Command tracking helps to determine whether the Control Manager successfully performs long-duration commands like virus pattern update and deployment.

On-Demand Product Control

The Control Manager provides you with real-time product control. Control Manager immediately carries out predetermined virus scan actions and applies configuration modifications made on the management console to the managed products. System administrators can run manual scans from the management console. This feature is indispensable during a virus outbreak.

Centralized Update Control

Centralized updates of spam rules, virus patterns, scan engines, and other antivirus and content security components ensure that all products contain the latest malware protection. You can view your entire network's protection status from a single management console.

Centralized Monitoring

Centralized monitoring gives you an overview of the antivirus and content security product performance using comprehensive logs and reports. The Control Manager collects logs from all its managed products; you do not need to check the logs of each individual product.

Control Manager tasks are different from ServerProtect tasks. ServerProtect tasks are customized, and saved for later use. Control Manager tasks are predefined and executed immediately. ServerProtect and Control Manager tasks can run simultaneously without interfering with each other.

Use the Control Manager Web-console to perform the following Control Manager tasks:

- Perform a manual scan (**Start Scan Now**).
- Enable a Real-time Scan.
- Deploy a virus pattern file/cleanup templates.

This command will deploy virus pattern, Damage Cleanup templates and Spyware pattern together.

- Deploy a scan engine file.

This command will deploy virus scan engine, Damage Cleanup Engine and 32bits Anti-Rootkit Driver.

Chapter 6

Registering and Contacting Technical Support

This chapter contains information to help you register and contact technical support.

The topics included in this chapter are:

Technical Support Information

A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current maintenance fees to have the right to continue receiving these services.

Evaluation copies of all Trend Micro products can be downloaded from the Trend Micro Web site.

Refer to the following online resources for technical support:

Email: sales@trendmicro.com

support@support.trendmicro.com

Web Support: http://esupport.trendmicro.com/support/smb

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

Virus Information Center: www.trendmicro.com/vinfo

Trend Micro Security Information

Comprehensive security information is available on the Internet at the Security Information section of the Trend Micro Web site:

www.trendmicro.com/vinfo/

Use Security Information to learn about:

- Computer virus hoaxes
- A weekly virus alert, listing the viruses that will trigger during the current week
- How to determine if a virus detection is a false alarm
- Trend Micro Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- Trend Micro virus reading room, with dozens of articles about the latest issues in computer viruses, including the threat posed by Java applets and ActiveX controls
- Product details and white papers

You can also access Trend Micro Virus Encyclopedia from the Management Console. Click **View** > **View Virus Encyclopedia** on the main menu.

Registering Trend Micro ServerProtect

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

To register ServerProtect visit the following Web site:

`www.trendmicro.com/support/registration.asp`

Using Knowledge Base

Trend Micro provides Knowledge Base, an online database filled with answers to technical product questions. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do.

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

New solutions are added daily. However, if you don't find the answer you seek, you can submit your question online, where the personnel at TrendLabs™ will provide you with an answer or contact you for more information.

Sending Trend Micro Your Viruses

ServerProtect detects infected files by means of pattern-matching (comparing files being scanned to the "fingerprints" of known viruses) and heuristics (monitoring the behavior of a file for tell-tale virus-like behavior). While these two methods are sufficient for most users, you also receive the support of Trend Micro antivirus engineers.

If you find a suspicious file (that is, ServerProtect does not identify it as a virus but you find that it exhibits strange behavior), or find a file that causes a "false alarm" (that is, you know that the file is not infected but ServerProtect identifies it as a virus), we invite you to send it to Trend Micro virus engineers for further analysis.

To submit a file to Trend Micro Virus Doctor:

1. Select a Normal Server on the domain name tree.
2. Click **Do** > **Submit File** on the main menu. The **Submit File** screen appears.
3. Type your name, company, phone and email address in the appropriate text boxes.

4. Type a brief description of the nature of the problem.

5. Type the name of the SMTP server that you want to use.

6. Click **Browse** to select the file you want to attach. The **Select File** dialog appears.

7. Select the file you want to submit, and then click **OK**.

8. Click **Submit** to send the message.

Our team of engineers will "dissect" the file to identify and characterize any virus(es) it may contain and return the cleaned file to you usually within 48 hours.

TrendLabs™

TrendLabs 24x7 global antivirus research and support centers form the backbone of Trend Micro service infrastructure. A team of more than 250 engineers operates around the clock at sites spanning the globe to keep customers informed and protected against the latest security threats. TrendLabs includes service centers in Tokyo, Paris, California, Taipei, Munich and its ISO 9002-certified headquarters in Metro Manila.

Appendix A

Converting the ServerProtect Trial Version and FAQs

A 30-day trial version of ServerProtect will be installed if no serial number is entered. This version will be fully functional but after 30-days virus scanning will be disabled. After this, you should either purchase the product or remove it.

After purchasing a license, refer to the following topics to update the serial number.

The topics included in this chapter are:

The Software Evaluation Period Window

If you install the trial version of ServerProtect, the **Software Evaluation Period** dialog appears every time you open the Management Console. The **Software Evaluation Period** dialog shows which Normal Servers are using the trial version and the number of days remaining until they expire.
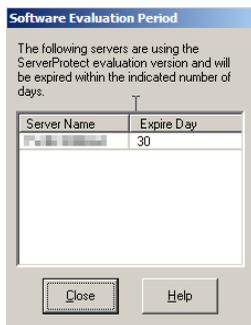
FIGURE A-1. Software Evaluation Period dialog

Viewing the Serial Number List

Using the Management Console, you can view the serial number of all the ServerProtect Normal Servers.

To view the serial number list:

1. Click **Help** > **About** on the main menu. The **About ServerProtect Management Console** dialog appears.

FIGURE A-2.   About ServerProtect Management Console dialog

2. Click **Serial Number**. The **Serial Number List** dialog appears showing you all the ServerProtect Normal Servers on your network, along with their respective serial numbers.
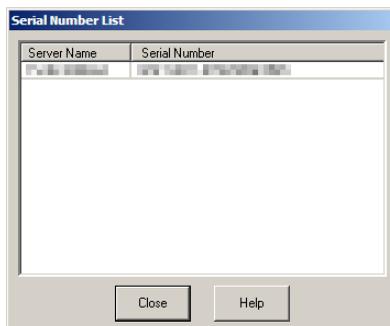
FIGURE A-3.   ServerProtect Serial Number List Window

3. Click **Close** to close the **Serial Number List** dialog, and then click **OK** to close the **About ServerProtect Management Console** dialog.

Updating a Serial Number

After you have purchased a ServerProtect license, you can update the serial number of installed ServerProtect software directly from the Management Console without reinstalling ServerProtect.

To update a serial number:

1. Select the Normal Server you want to update the serial number for in the domain browser tree.

2. Click **Do** > **Update Serial Number** on the main menu. The **Enter New Serial Number** dialog appears.

FIGURE A-4. Enter New Serial Number dialog

3. Type the new serial number in the **New serial number** text boxes.

4. Click **OK**. Otherwise, click **Cancel** to close the dialog.

Frequently Asked Questions (FAQs)

Virus Scan for NetApp Filer

- **Why ServerProtect can not detect viruses in NetApp filer but can detect them in other locations?**

  File extensions that you want to scan for viruses are need to be specified on NetApp filer. You can check the current registered file extensions using command `vscan` on NetApp Filer's console.

- **Why ServerProtect scan the directories/files that I have already added to Exclusion List?**

  ServerProtect scans all the files that are requested by NetApp Filers, even if the directories/files are added to Exclusion List on NetApp Filers.

- **Why I cannot scan any virus on filer even though I am connected to the filer?**

  Check whether **Vscan** is enabled on NetApp Filers or not. Enabling **Vscan** also enables scanning for viruses on all Vfilers.

- **How can I enable scanning for viruses on each Vfiler?**

  Check whether **Vscan** is enabled on NetApp Filers or not. Enabling **Vscan** also enables scanning for viruses on all Vfilers.

Upgrading ServerProtect

- **I have already migrated Management Console from 5.62 to 5.8 but Management Console is not working properly, what should I do?**

  Check the version of your Information Server. The ServerProtect version used for the Management Console and Information Server must be the same. ServerProtect 5.8 Management Console cannot be used to manage ServerProtect 5.62 Information Server or vice versa.

  We also recommend you to migrate all Normal Servers to version 5.8. The ServerProtect version installed on Normal Server should be same or higher than the Information Server managing them. ServerProtect 5.8 Management Console cannot modify task settings for ServerProtect 5.62 Normal Servers.

- **Can I rollback ServerProtect from 5.8 to 5.62?**

  No. You cannot rollback ServerProtect to the previous version after the upgrade.

- **I have installed ServerProtect 5.62Management Console and ServerProtect 5.62 Normal Server on the same server computer. Can I use deployment program to upgrade them separately?**

  No. If the Normal Server and Management Console are installed on the same server computer, the deployment program will upgrade them together.

- **Can I upgrade ServerProtect 5.31 to 5.8 from Management Console?**

  No. The upgrade from Management Console is not supported for ServerProtect version lower than 5.8. Alternatively, you can remove the existing ServerProtect version and install ServerProtect 5.8 from the setup program.

- **Can I use installation package to remotely migrate the existing Management Console?**

  No. The remote migration/installation is not supported for Management Console. The Management Console does not get an upgrade during remote installation/migration.

Note: To receive the latest virus protection, it is highly recommended to update your virus pattern files and virus scan engine immediately after the installation. Also, you should modify the default Deploy task, and add the Spyware pattern, Virus Cleanup Template, Virus Cleanup Engine, and Anti-rootkit Driver as the update components.

ServerProtect Virus Scan

- **Why the file name and file path in Scan Result are not displayed correctly and appears to be truncated; and the Restore button is inactive?**

  The entry field for the file name and file path in **Scan Result** window can display the file name (including file path) up to 256 characters. If it exceeds 256 characters, the file name or file patch will be truncated and the Restore button will be inactive.

- **Why the Deny White List does not work?**

  The Deny White List does not work if Real-time Scan is disabled. Enable the Real-time scan to activate Deny White List.

- **Why the pop-up notification messages do not appear, even though I have set the alert method to display pop-up message box for notifications?**

  If the **Messenger** service is not activated on Windows Server 2003, the pop up messages will not appear. However, Windows Server 2008 does not support the **Messenger** service. Therefore, the pop-up message notifications will not work on Windows Server 2008.

- **Why the Result in Log detail information shows the virus as cleanable, even if it is not a cleanable virus?**

  If the **Action** is set to **Clean** in the **Set Action** window, the virus will be correctly shown as cleanable or uncleanable. However, if the **Action** is not set to **"Clean"**, the virus will always be shown as cleanable in Log detail information.

Miscellaneous

- **Why there are old logs in Control Manager when installing CMAgent? Where did they come from?**

  After Control Manager agent is installed, ServerProtect sends all pre-existing logs to the Control Manager Server. However, this may generate additional network traffic. To avoid redundancy, purge all logs from the Management Console before installing the CMAgent.

- **I have installed Information Server in the computer system, which is having multiple network cards belonging to different network segments. Why the Information Server could not be displayed in the Information Server list when Management Console is open, and the link between Information Servers and Normal Servers is broken?**

  The Information Server could not be displayed in the Information Server list because when Information Server/Normal Server attempts to connect to the correct network, it could not reach the network. To resolve the problem, uninstall both the Information Server and the Normal Server and reinstall them

- **Why I can not see the Normal Server's icons in the system tray?**

  If you use a remote desktop connection, the Normal Server's icons may not be displayed in the system tray.

- **Why I cannot see the Pattern and Engine of Normal Server?**

Normal Server Pattern and Engine and other related information will not displayed in the Management Console if the Normal Server is disconnected from the Information Server. A cross sign will be displayed in the Management Console status window if the link between Normal Server and Information Server is broken.

• **If I enable "ExcludeUNCPath" in Admin.ini, will ServerProtect exclude User Access Control (UNC) path in all environments?**

The ServerProtect may not exclude User Access Control (UNC) path in Windows Server 2008 even though **ExcludeUNCPath** is enabled in Admin.ini.

• **I have installed ServerProtect 5.8 on Windows Server 2003. Why ServerProtect displays the login failure error if the password is blank?**

Since Windows Server 2003 has user account restriction, users' password must be set; the ServerProtect displays login failure error if the password field is blank and password is not set.

Index