TREND MICRO

TREND MICRO™ ServerProtect5

Comprehensive virus protection for enterprise-class servers and storage systems

for Windows Server 2003/Storage Server 2003

Getting Started Guide

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 Website 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

Document Part No. SPEM51426/30407

Release Date: June, 2007

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

Chapter 3: Managing ServerProtect

Chapter 1

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 Windows™ Storage Server 2003/Server 2003 from a single portable management console. The console enables administrators to configure servers in the same domain simultaneously and to generate integrated virus incident reports from all of them.

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

The topics included in this chapter are:

- How Does ServerProtect Work?
- ServerProtect Architecture
- Real-time Scan vs. On-demand Scan (Scan Now)

- Working with Tasks
- When SeverProtect Finds a Virus (Virus Actions)
- Virus Logs
- Deploying Updates
- ServerProtect Virus Detection Technology
- Additional Features

How Does ServerProtect Work?

ServerProtect monitors all activity on Windows Storage Server 2003/Server 2003. Whenever it 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 lets you 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 the system's components. Management Console instructions are sent to the Information Server, which then passes them on to the Normal Servers.

Communication Methods

The Management Console uses Transmission Control Protocol/Internet Protocol (TCP/IP) with password-protected logon to communicate with the Information Server. The Information Server uses Remote Procedure Call (RPC) to connect to Windows Storage Server 2003/Server 2003 servers.

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:

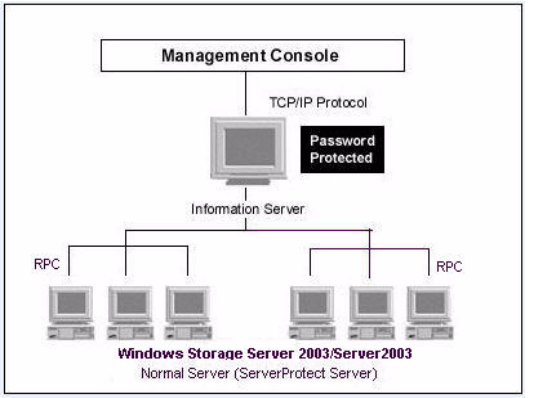


FIGURE 1-1. ServerProtect Three-tier Architecture

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 servers in the same domain and generate integrated virus incident reports for all servers. The console has the following parts:

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

Note: Only one Management Console can manage an Information Server. This means once a Management Console is connected to an Information Server, no other Management Console can connect to it.

The ServerProtect domain browser tree shows all the ServerProtect servers installed on Windows Storage Server 2003/Server 2003 servers with the status of each server. Status information includes: the version of the virus pattern and scan engine file, type and version of operating system, 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 multiple Normal Servers. See *Installing a Normal Server* on page 2-17.

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 may, 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.

ServerProtect offers several ways for installing Normal Servers:

- Using the setup program. See *Installing a Normal Server from the setup program* on page 2-17.
- Using the Management Console. See *Installing a Normal Server from the Management Console* on page 2-20.
- Using Microsoft Server Management Server (SMS). See *Deploying through Microsoft SMS* on page 2-22.
- Using silent mode. See *Installing ServerProtect in Silent Mode* on page 2-31.

Each of the listed installation methods can be tailored to your specific company needs. See *Installing a Normal Server* on page 2-17.

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

WARNING! *Since 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 your network's protection is to group all servers in relevant ServerProtect domains. For example, you may create a ServerProtect domain called "NS" to manage Normal Servers more efficiently. See *Managing ServerProtect Domains* on page 3-8.

WARNING! *ServerProtect domains are not the same as Windows Storage Server 2003/Server 2003 domains; they are 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**: Once logged on to the console, IT professionals can add, rename, or move/delete domains according to their preference.

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 3-49.

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 3-52.

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. However, 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 reliably, while minimizing the impact on system resources. See *Scanning Viruses* on page 3-45.
- **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 3-45.

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, Delete, 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 3-27.

Once 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 definition.

When ServerProtect Finds a Virus (Virus Actions)

ServerProtect lets you configure the kind of action that the software takes on infected files. You can even choose different courses of action for different kinds of viruses.

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 3-45 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. Since 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 3-45.

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.

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.

The default size for the log file is 8000 entries, or up to 10MB. Once the log file exceeds 8000 entries or 10MB, ServerProtect automatically renames the log file and creates a new log file.

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, please 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 3-14.

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

ServerProtect update features include:

- **Update component selection:** You can update a pattern and scan engine.
- **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 roll-back a deployed pattern and scan engine file to the previous version.

Note: ServerProtect 5.7 does not support 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 3-17.
2. Deploy the downloaded updates to other Normal Servers on the network. See *Deploying Updates* on page 3-23.

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 3-29.

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 virus action you previously specified. 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 3-45.

Note: It is important to keep the virus pattern file 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 Download* on page 3-19 and *Configuring a Scheduled Deployment* on page 3-24 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. Since they are harbored in files that are commonly passed around via email, these kinds of viruses are easily spread. See *Configuring Real-Time Scan* on page 3-49 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 via email and the Internet. Since some antivirus software are 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) & PKZIP_SFX (.exe)
- LHA (.lzh) & LHA_SFX (.exe)
- ARJ (.arj) & 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 Real-Time Scan* on page 3-49, and *Configuring Scan Now* on page 3-52.

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.

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 sheet, and in turn this Excel 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" which complements state-of-the-art ServerProtect virus protection. See *Scanning Viruses* on page 3-45.

Tip: OLE layer scan offers five layers of protection. Trend Micro recommends a setting of 2 OLE layers for Scan Now and a setting of 1 for 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 (i.e. txt), IntelliScan will use the file header to verify the true file type. See *Scanning Viruses* on page 3-45.

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**: Since 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 3-52.

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 3-45.

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 Real-Time Scan* on page 3-49.

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 multiple Windows Storage Server 2003/Server 2003 servers on your network. The console is portable and can be run on any 32-bit/64-bit Windows server (except Windows NT 3.51).

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.

Faster Response to Virus Outbreaks

If a virus tries to infect a file in a shared folder on a server running ServerProtect, a message box appears notifying which computer the virus originated from on a network. This message box also displays the following information: type of scan, the name of the virus, File, Computer, and User. In addition, it also displays the action taken on the virus and the source of infection. See *Configuring Notification Messages* on page 3-39.

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 via 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 Storage Server 2003, and Microsoft Windows Server 2003 servers. It also supports Network File System (NFS) drivers, and SOCKS 4 for Trend Micro update server.

ServerProtect is compatible with 32-bit operating systems and 64-bit operating systems. ServerProtect will automatically detect 32-bit and 64-bit Windows Storage Server 2003 and Windows Server 2003. If the operating system is 32-bit, then 32-bit binaries of the Normal Server component of ServerProtect will be installed/uninstalled. If the operating system is 64-bit, then 64-bit binaries of the Normal Server component of ServerProtect will be installed/uninstalled.

Chapter 2

Installing ServerProtect

This chapter includes the necessary information to successfully install ServerProtect on your network(s).

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

The topics included in this chapter are:

- Recommended System Requirements
- Installation Scenarios
- Installing ServerProtect
- Removing ServerProtect

Recommended System Requirements

The recommended system requirements are different for each ServerProtect component.

Normal Server

- 2.5GHz Intel™ Pentium™ IV processor or 3.0GHz EM64T Intel™ processor or 2.0GHz AMD Athlon™ 64-bit processor (or equivalent)
- Operating System:
    - Microsoft Windows Storage Server 2003.

      Minimum 512MB RAM, recommended 1GB RAM
    - Microsoft Windows Server 2003.

      Minimum 256MB RAM, recommended 512MB RAM
- 120MB of free disk space
- The following network protocols and services must be installed: TCP/IP, Microsoft Network, and RPC services must be running on Windows Storage Server 2003/Server 2003 Workstation.

Information Server

- 3.0GHz Intel™ Pentium™ IV processor or 3.0GHz EM64T Intel™ processor or 2.0GHz AMD Athlon™ 64-bit processor (or equivalent)
- Operating System:
    - Microsoft Windows Storage Server 2003.

      Minimum 1GB RAM
    - Microsoft Windows Server 2003 Server.

      Minimum 512MB RAM, recommended 1GB RAM
- 120MB free disk space
  140MB free disk space if installing with Control Manager agent

---

Note: For Active Update 2.8, an additional 300MB free disk space is required if Smart Duplicate is turned on and the cached pattern number is set to 7.

- The following network protocols and services must be installed: TCP/IP, Microsoft Network, NetBIOS Compatible Transport Protocol, and RPC services.

Management Console

- 2.5GHz Intel™ Pentium™ IV processor or 3.0GHz EM64T Intel™ processor or 2.0GHz AMD Athlon™ 64-bit processor (or equivalent)
- Operating System:
    - Microsoft Windows Storage Server 2003.

      Minimum 512MB RAM, recommended 1GB RAM
    - Microsoft Windows Server 2003.

      Minimum 256MB RAM, recommended 512MB RAM
- A monitor with 1024x768 or higher resolution
- The following network protocols and services must be installed: TCP/IP, Microsoft Network, and RPC Services.

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 2-5.

Specifying Your Installation Environment

Trend Micro ServerProtect supports Windows Storage Server 2003 and Windows Server 2003 servers/workstations. 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 1-7.

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 1-5.

The following table shows the different installation environments for each ServerProtect setup component.

ServerProtect Setup Component	Windows Server 2003 (32-bit)	Windows Storage Server 2003 (32-bit)	Windows Server 2003 (64-bit)	Windows Storage Server 2003 (64-bit)
Information Server	Yes	Yes	Yes(WOW64)	Yes(WOW64)
Normal Server	Yes	Yes	Yes	Yes
Management Console	Yes	Yes	Yes(WOW64)	Yes(WOW64)

TABLE 2-1. ServerProtect Installation Environments

A Windows Storage Server 2003/Server 2003 Environment

If you are installing ServerProtect for the first time, and all the servers on your network are running Windows Storage Server 2003/Server 2003, the installation is quite straight forward.

To deploy ServerProtect in a Windows Storage Server 2003/Server 2003 environment:

1. Install the Information Server. See *Installing an Information Server* on page 2-14.
2. Install the Normal Server on the Information Server computer. See *Installing a Normal Server from the setup program* on page 2-17.
3. Install the Management Console on the Information Server computer. See *Installing the Management Console* on page 2-11. You can install additional Management Consoles on any Windows Storage Server 2003/Server 2003 computer connected to your network.

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

4. Update ServerProtect pattern and scan engine files. See *Configuring Updates* on page 3-14.
5. Create additional ServerProtect domains to manage your Normal Servers. See *Creating ServerProtect Domains* on page 3-8.
6. Install the remaining Windows Storage Server 2003/Server 2003 Normal Servers using the Management Console. See *Installing a Normal Server from the Management Console* on page 2-20.

Steps 1, 2 and 3 can be executed simultaneously during 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 installing Information Servers in the same physical segment of the network as the Normal Servers they manage.

For example, if you want to manage ServerProtect Normal Servers in Japan from a Management Console in Germany, we recommend the Information Server(s) managing the Normal Servers is also in Japan.

Note: To ensure proper network performance install ServerProtect Information Servers in the same physical segment of the WAN as the Normal Servers they manage.

Since 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

If you are installing ServerProtect for the first time, Trend Micro recommends installing a complete ServerProtect package, including the Management Console, Information Server, and Normal Server.

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.

It is also good practice to install the program on a test server first, so that installation issues, if any, can be worked out before installation on production servers. Before installing ServerProtect, make sure you carefully read the Installation Scenarios section. See *Installation Scenarios* on page 2-4.

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 Normal Server execute the setup program on a Windows Storage Server 2003/Server 2003 server/workstation computer.

To install the complete ServerProtect package:

1. Insert the Enterprise CD-ROM and run `SETUP.EXE`. The ServerProtect **welcome** screen appears.

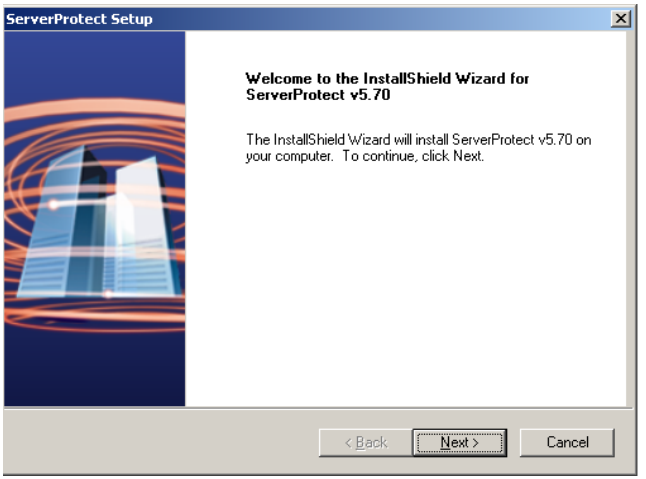


FIGURE 2-1. ServerProtect Welcome screen

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

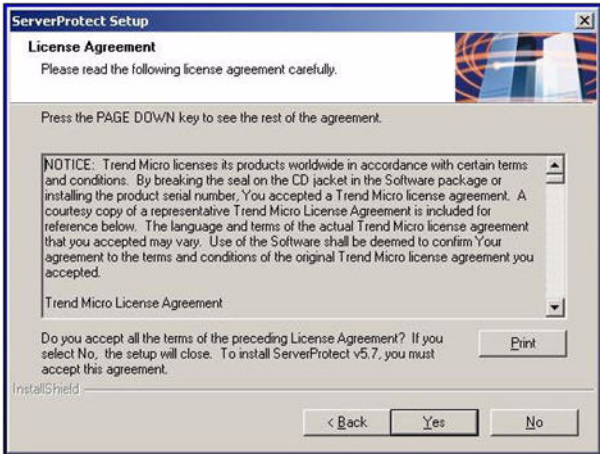


FIGURE 2-2. Software License Agreement screen

3. Click **Yes**. ServerProtect checks your boot sector for viruses.

FIGURE 2-3. Scan Result Information window

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

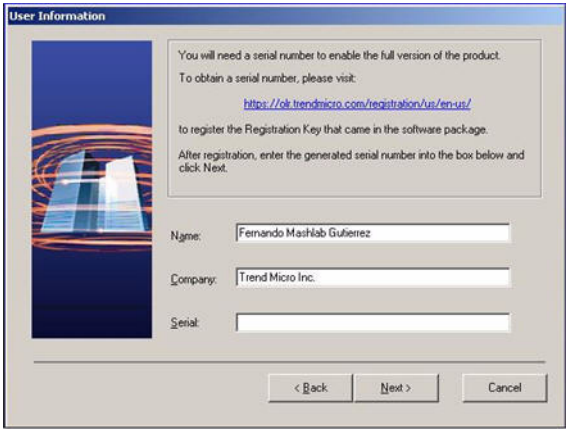


FIGURE 2-4. ServerProtect User Information screen

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

   If you do not have the serial number, you can leave the field blank and a 30-day trial version will be installed instead. If you enter an incorrect serial number, an "Incorrect serial number entered" message will appear.

6. Click **Next** to continue the setup. The **Select Components** screen appears.

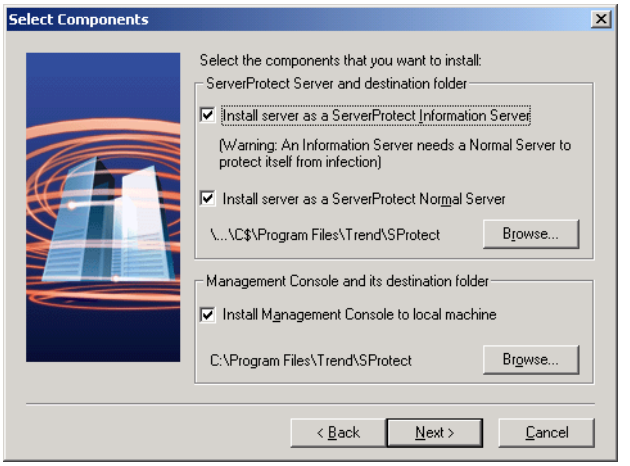


FIGURE 2-5. ServerProtect Select Components screen

7. Select the check boxes for the components you want to install. Make sure you select the adequate components for the desired setup. You can choose hidden share drives, e.g., 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 same computer.

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, and then click **Next**.

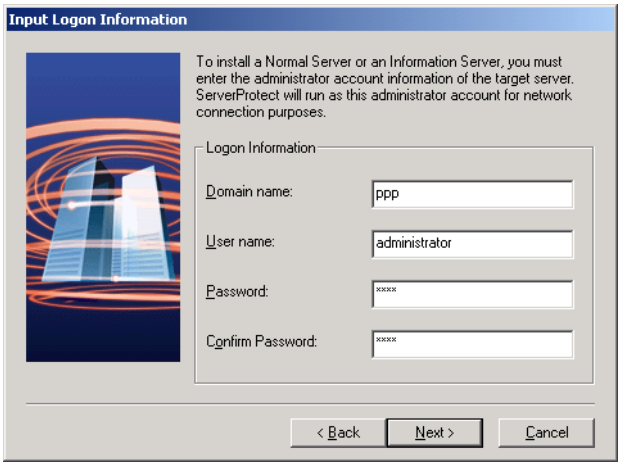


FIGURE 2-6. Input Logon Information screen

9. Follow the instructions to complete the ServerProtect Setup.

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 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. See Figure 2-5. You can change the local installation path by clicking **Browse**. The Management Console must be installed in a Windows Storage Server 2003/Server 2003 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** window 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.

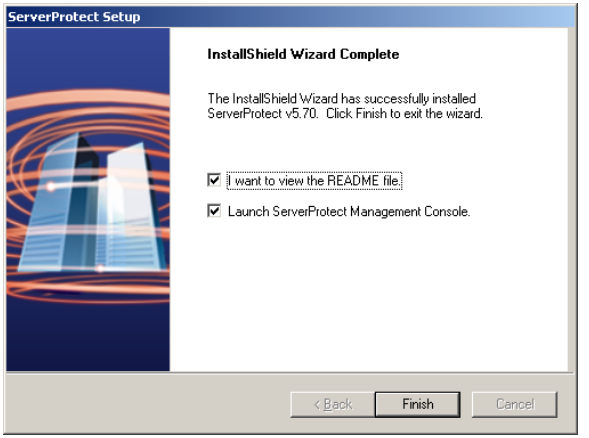


FIGURE 2-7. ServerProtect Setup Complete screen

5. Click **Finish**. The **Select an Information Server** window appears.

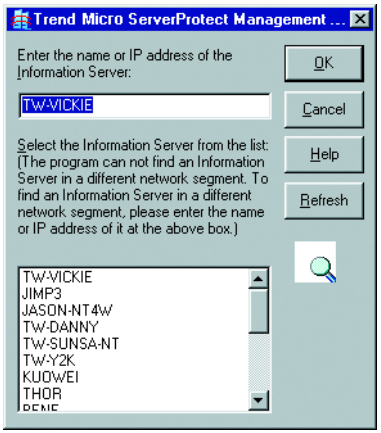


FIGURE 2-8. Select an Information Server screen

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 window without saving.

Installing an Information Server

The Information Server manages Normal Servers and responds to commands issued by the Management Console.

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 **Select Components** screen. See Figure 2-5.

   Click **Browse** to locate the target server and folder where you want to install an Information Server. The **ServerProtect Install Path Selection** window appears.

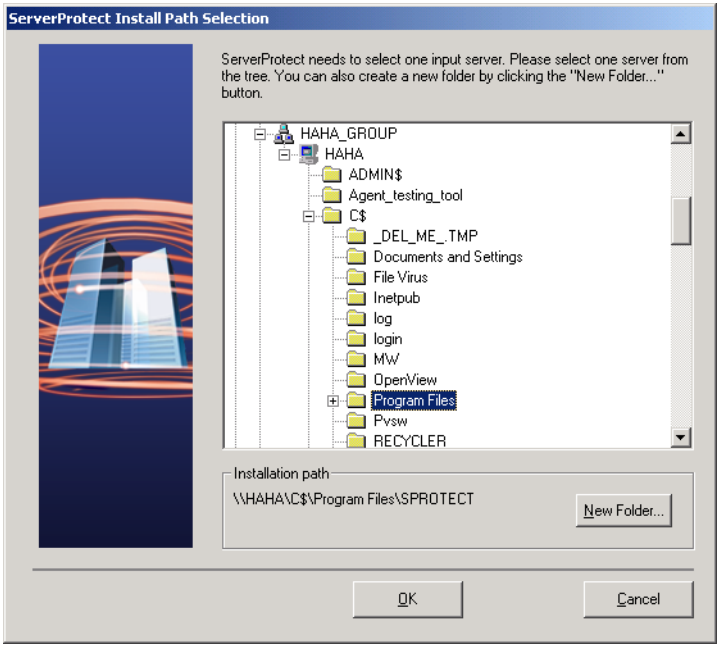


FIGURE 2-9. ServerProtect Install Path Selection screen

3. Double-click the target server and choose the installation path for ServerProtect Information Server files. To create a new folder, click **New Folder** and then click **OK**.
4. Click **Next** in the **Select Components** screen. The **Input Logon Information** screen appears. See Figure 2-6.
5. Under **Logon Information,** type the appropriate data in the **Domain name**, **User name**, **Password**, and **Confirm Password** fields, and then click **Next**.

   The ServerProtect **Setup Information Server** screen appears.

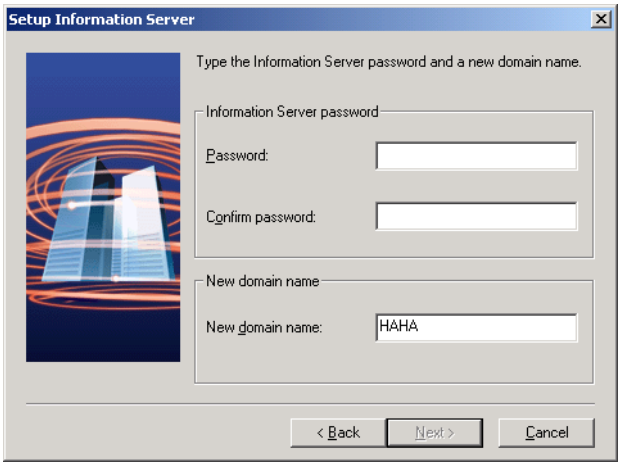


FIGURE 2-10. ServerProtect Setup Information Server screen

6. Type a password. This prevents unauthorized access to this Information Server from either the Management Console or the setup program.
7. Click **Next**. The **Start Copying Files** window 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.

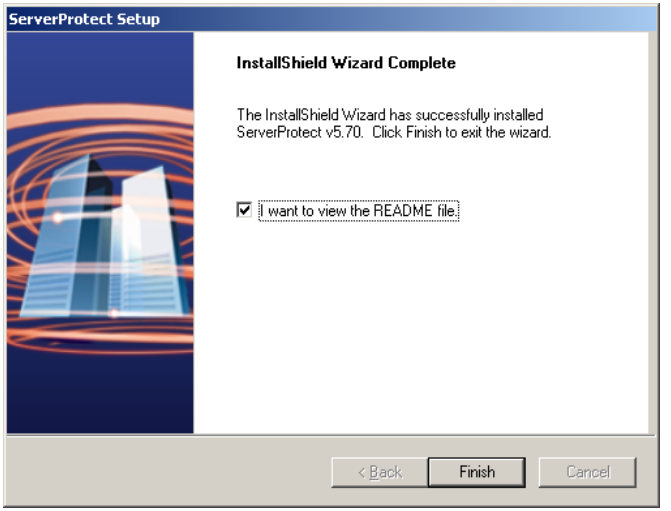


FIGURE 2-11. ServerProtect Setup Complete screen

9. Click **Finish.** The **Install Control Management Agent now** screen appears.

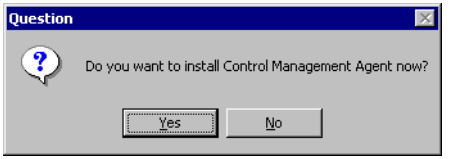


FIGURE 2-12. Control Manager Agent Installation window

10. Click **Yes** to install the Control Manager agent; otherwise, click **No** to close the setup 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 your network.

Note: The Normal Server can only be installed on a Windows Storage Server 2003/Server 2003.

To install a 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 Figure 2-5.

   Click **Browse** to locate the target server and folder where you want to install a Normal Server. The **ServerProtect Install Path Selection** window appears.

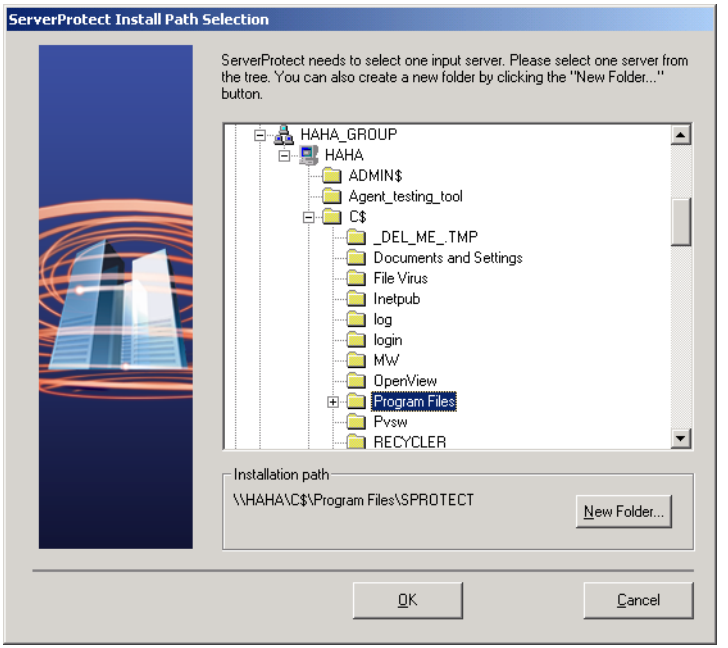


FIGURE 2-13. ServerProtect Install Path Selection screen

3. Click the appropriate network to expand the tree, and then click the target server.
4. Click **OK**. The **Enter Password** window appears.

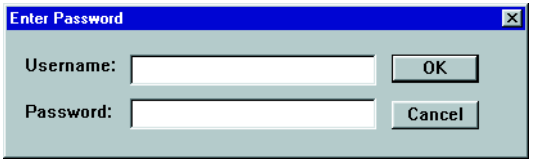


FIGURE 2-14. ServerProtect Target Server Logon window

5. Type an administrator user name and password to access the target server, and then click **OK**. The target server's local drives appear on the tree.

6. Select the installation path for your Normal Server, and then click **OK**. To create a new folder, click **New Folder** and then click **OK**.
7. Click **Next** in the **Select Components** screen. The **Input Logon Information** screen appears.
8. Under **Logon Information**, type the appropriate data next to the **Domain name**, **User name**, **Password**, and **Confirm Password** fields.
9. Click **Next**, the **ServerProtect Installation Path Selection** screen appears.

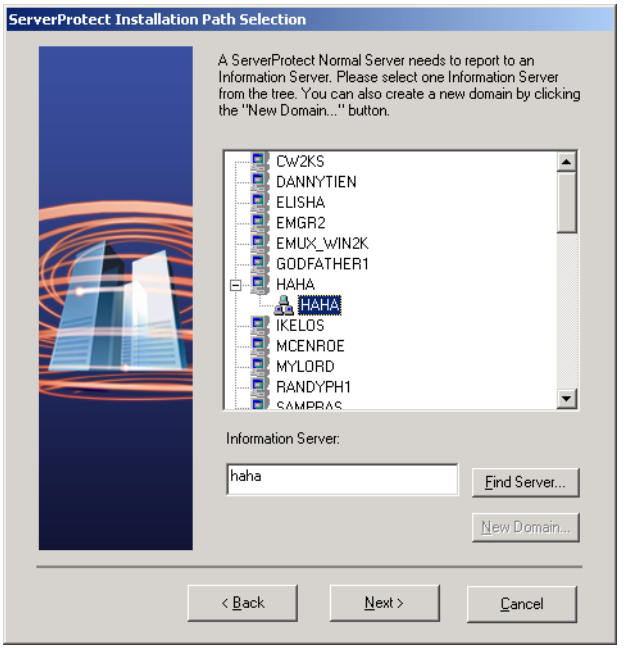


FIGURE 2-15. The ServerProtect Installation Path Selection screen

10. To locate an 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.

    Click **New Domain** if you want to create a new ServerProtect domain.

Note: If an Information Server resides on a network different from that of the Normal Server, the server may not appear in the list. In this case, it may be necessary to type its server name or the IP address in the **Information Server** field to locate it.

11. Click **Next**. The **Input ServerProtect Information Server password** screen appears.
12. Type the Information Server password, and then click **OK**. This password was assigned during Information Server installation.

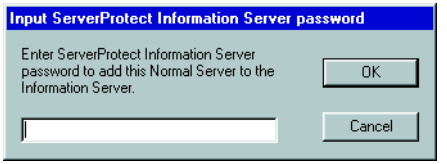


FIGURE 2-16. Input ServerProtect Information Password window

The **Start Copying Files** window appears. Verify the information listed on the screen.

13. 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. See Figure 2-11.
14. Click **Finish**. A ServerProtect icon ( ) will be added to your Windows taskbar, notifying you that the scanner is on.

Installing a Normal Server from the Management Console

The Information Server the Management Console is logged on to, should already be managing at least one Normal Server. The existing 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 will be installed. For example, Windows Storage servers need a Windows Storage source.

If there is only one existing Normal Server of the same type as the server to be installed shown in the server tree, it is automatically selected as the source server.

To install a Normal Server from the Management Console:

Note: While installing a 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.

---

1. From the domain browser tree, select the domain to which you want to add a server.
2. 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** window opens.
3. Select an existing Normal Server from the list box, and then click **OK**. A confirmation window appears.
4. Click **OK**. The **Add Server(s) to Domain** window opens.
5. Do one of the following to add a server to the domain:
   - Select the server name in the left-hand list box
   - Type the server name in **Server name**
6. Click **Add** to enter the server name into the right-hand list box.
7. Repeat step 5 until the right-hand list box displays all the servers that you want to add into the new domain. If you want to remove a server that you have previously added, highlight the name in the right-hand list box and click **Remove**. Click **Remove All** to clear the right-hand list box.

8. Click **OK** to save your changes or click **Cancel** to close the window without adding a server.

   Note: If the operating system of the source and the target servers are of different platforms, then a "Failed to complete this operation" message will appear when you click **OK**. In the event log, the message "you cannot install a new ServerProtect from 32-bit source server on a 64-bit target server and vice versa" will appear.

Note: Adding and installing a Normal Server are two different operations. In the former, you are merely transferring an existing Normal Server from one Information Server to another. In the latter, you are registering a new Normal Server by remotely installing the software.

Deploying through Microsoft SMS

You can install ServerProtect through Microsoft Systems Management Server (SMS) 2003 on a Windows Storage Server 2003/Server 2003 platform.

Note: You must install the Microsoft SMS software on your Windows Storage Server 2003/Server 2003 server to deploy client software through SMS.

The deployment procedures listed below illustrate how to deploy ServerProtect through Microsoft SMS 2003.

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** window appears.

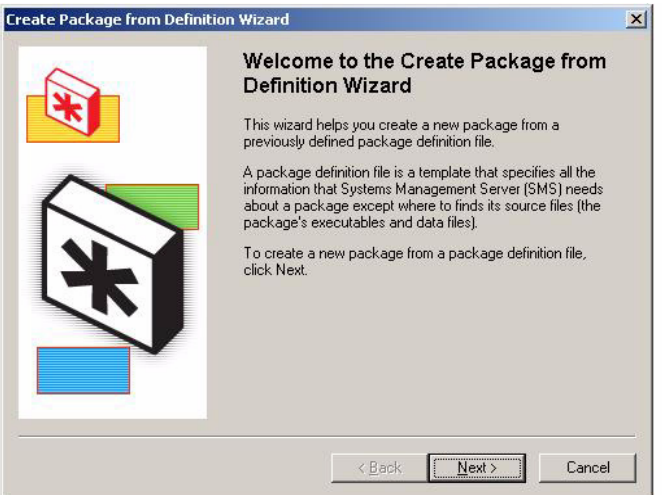


FIGURE 2-17. Create Package from Definition Wizard window

4. Click **Next**. The **Package Definition** window appears.

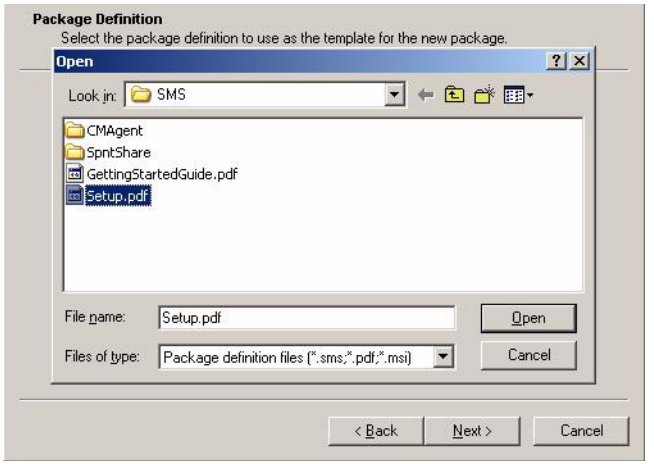


FIGURE 2-18. File Browser window

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** window.

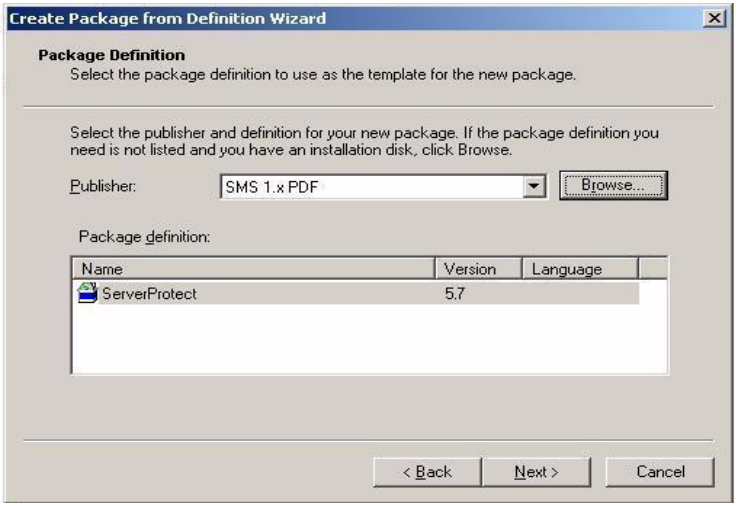


FIGURE 2-19. Package Definition window

6. Click **Next,** the **Source Files** window appears**.**

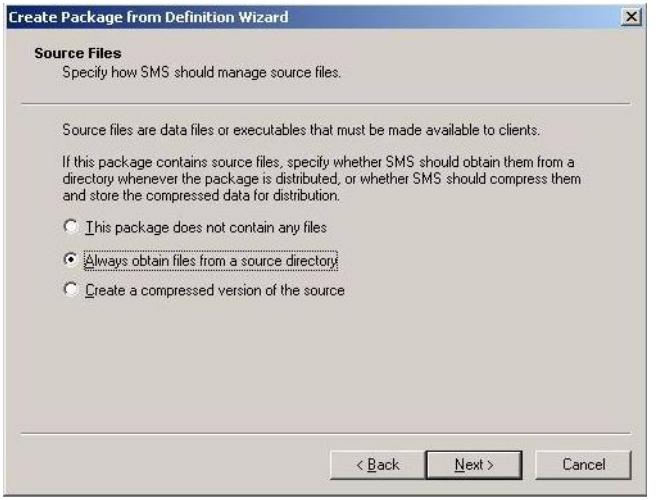


FIGURE 2-20. Source Files window

7. Select the **Always obtain files from a source directory** option and click **Next**. The **Source Directory** window appears.

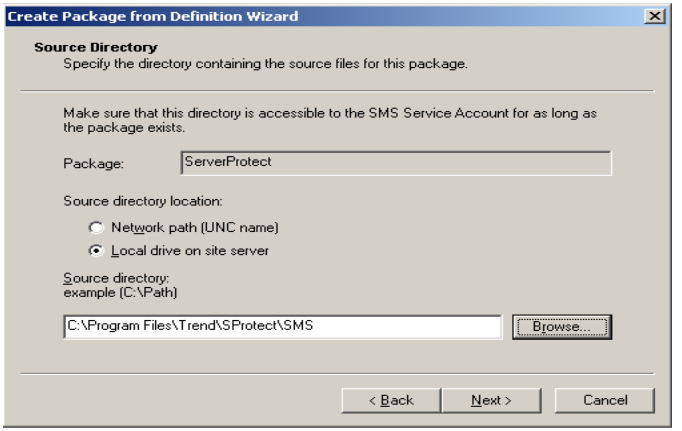


FIGURE 2-21. Source Directory window

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** window appears.

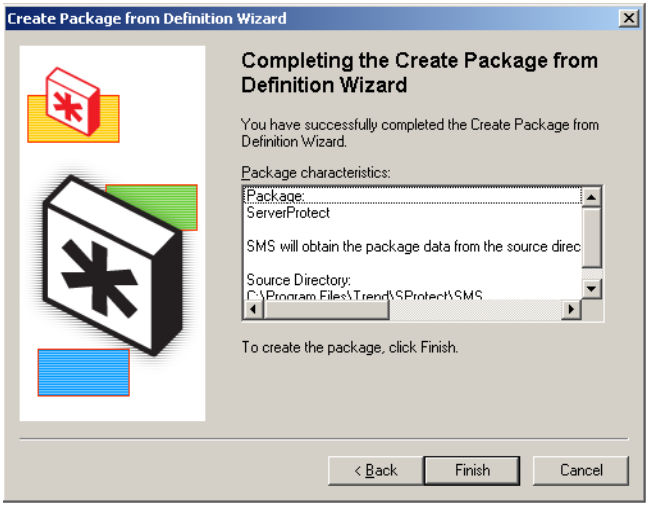


FIGURE 2-22. Completing the Create Package from Definition Wizard window

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.

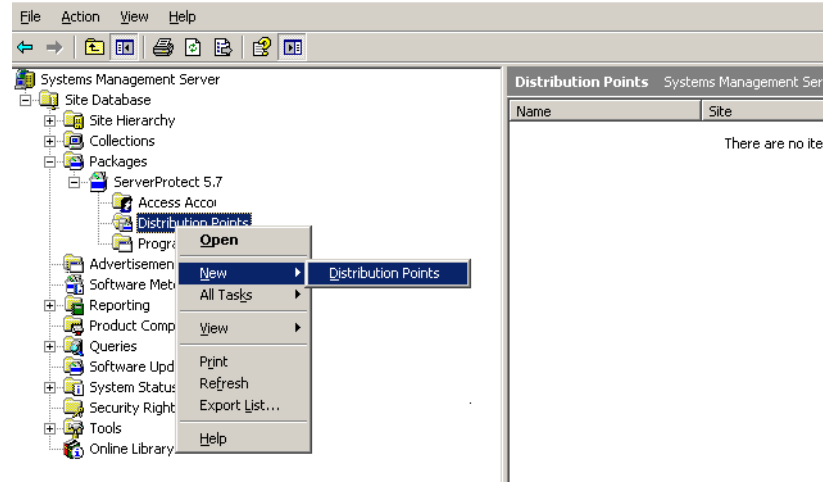


FIGURE 2-23. SMS Administrator window

12. Right-click **Distribution Points** and select **New** > **Distribution Points**. The **Copy Package** window appears.

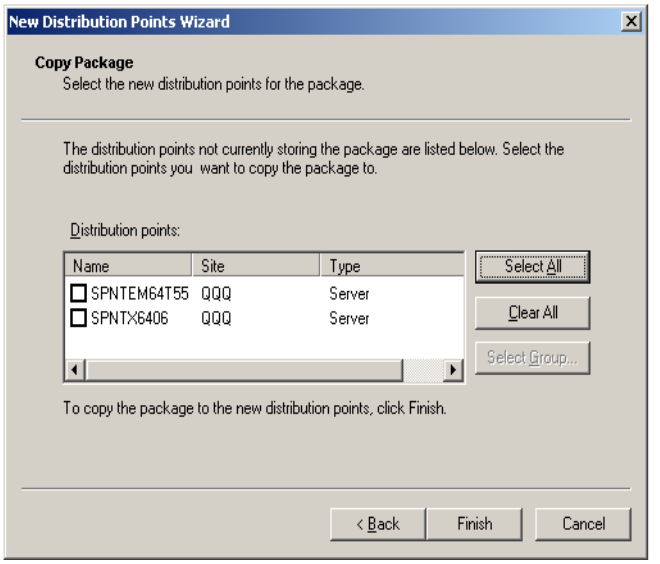


FIGURE 2-24. Copy Package window

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** window appears.

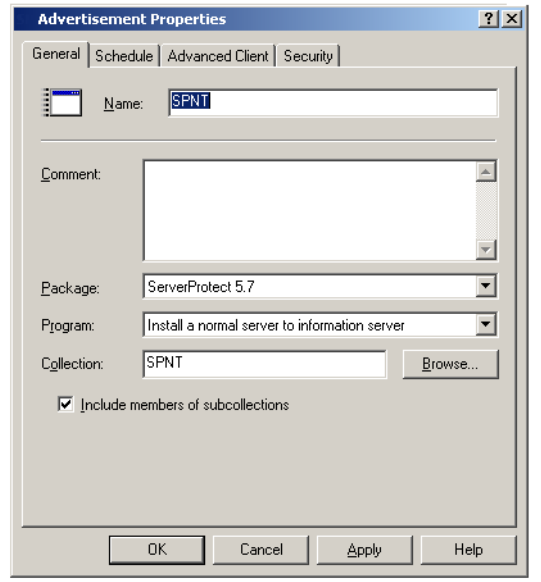


FIGURE 2-25. Advertisement Properties window

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/workstations collection.

Installing ServerProtect in Silent Mode

Installing ServerProtect in silent mode can be quite useful to remotely install Windows Storage Server 2003/Server 2003 Normal Servers.

To install ServerProtect in silent mode for Windows Storage Server 2003/Server 2003:

1. Install an Information Server. See *Installing an Information Server* on page 2-14.
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"SPNT5"
   ```

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"SPNT5"
   ```

   e. Press **Enter**.

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

For 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 from a Windows Storage Server 2003/Server 2003 environment:

To remove a Normal Server remotely for Windows Storage Server 2003/Server 2003:

1. Click a Normal Server from the Management Console.
2. Click **Domain** > **Uninstall ServerProtect** from the main menu.

   All selected servers will be remotely removed.

To remove a Normal Server locally for Windows Storage Server 2003/Server 2003:

1. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
2. Click **Normal Server**, and then click **Remove**.

Removing an Information Server

The Information Server Service can only be removed locally.

To remove an Information Server for Windows Storage Server 2003/Server 2003:

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 Windows Storage Server 2003/Server 2003:

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
- Managing ServerProtect Domains
- Managing Information Servers
- Managing Normal Servers
- Deploying Updates
- Managing Tasks
- Configuring Notification Messages
- Scanning Viruses
- Using Real-time Scan
- Using Scan Now (Manual Scan)
- Scheduled Scanning

Using the Management Console

ServerProtect lets you manage multiple Windows Storage Server 2003/Server 2003 servers and workstations from a single, portable Management Console running on any 32-bit or 64-bit Windows server. The console is password protected, to ensure that only authorized administrators can modify the settings of ServerProtect.

Opening the Management Console

You can run the Management Console from any 32-bit or 64-bit Windows server 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 3-1. Trend ServerProtect Management Console Logon window

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

2. Type the administration password defined during Information Server installation, and then click **OK**. Note that the password is case-sensitive and you can only log on to one Information Server at a time.

Management Console Main View

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

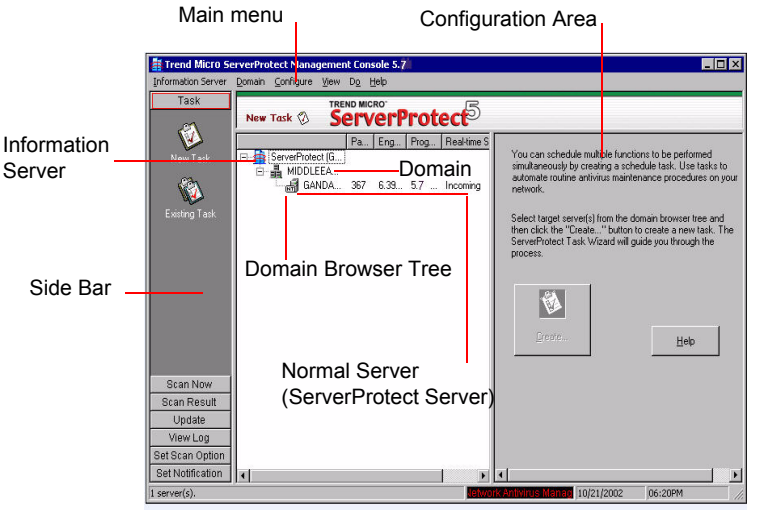


FIGURE 3-2. Management Console Elements

The Management Console has the following components:

- Main menu
- Side bar
- Domain browser tree
- Configuration Area

Main Menu

The Main menu at the top of the screen includes six items:

- **Information Server**: To configure the information about Information Server. For example, to back up or restore IS information and to select or move the Information Server on the network.
- **Domain**: To change the domain and server organization shown on the domain browser tree
- **Configure**: To modify the scanning and log file configuration, and to set console refresh frequency
- **View**: To view ServerProtect log files, scan results, and the Trend Micro Virus Encyclopedia
- **Do**:
  - To create or modify tasks
  - To perform on-demand scans
  - To update or roll back virus pattern and scan engine
  - To change the IS password
  - To find domains or servers
- **Help**: To access the online help system and 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: To create a new task

Existing Task List: To view, run, modify, or delete an existing tasks

Scan Group

Scan Now: To configure a manual virus scan

Scan Result Group

Real-time Scan: To view the result of a real-time scan

Scan Now: To view the result of a manual scan

Task Scan: To view the scanning result performed by a task

Update Group

Update: To download and deploy updates to the Normal Servers located on the network

Rollback: To roll back to a previous deployment action performed on your network

View Log Group

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

Set Scan Action Group

Real-time Scan: To configure a real-time virus scan on the network

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

Deny Write List: To prevent certain files or directories from modification

Notification Group

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

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

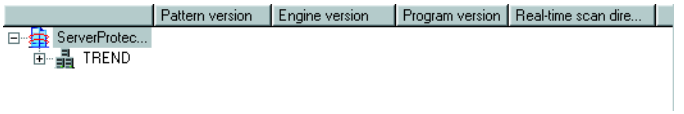
Domain Browser Tree

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

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 Windows Storage Server 2003/Server 2003 Normal Server

 An infected Windows Storage Server 2003/Server 2003 Normal Server

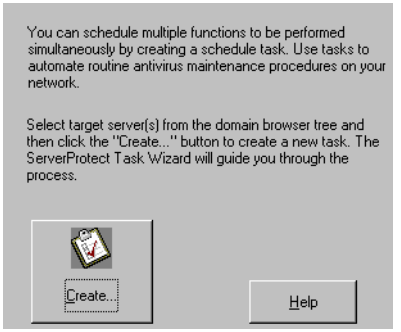
 A Normal Server that has been disconnected or its service has been disabled

 A Normal Server in Outbreak Prevention Policy mode

 An infected Normal Server 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.



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 seem to be on fire. This is to remind you to scan the infected server and prevent the virus from spreading throughout your network. To remove the infection icon(s), you need to purge all log entries under **Scan Result** in the Management Console.

Creating ServerProtect Domains

After creating a default domain via 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:
   - Click **Domain** > **Add New Domain** on the main menu.
   - Right-click the Information Server icon on the domain browser tree and then click **Add New Domain**.

   The **Create New Domain** window appears.

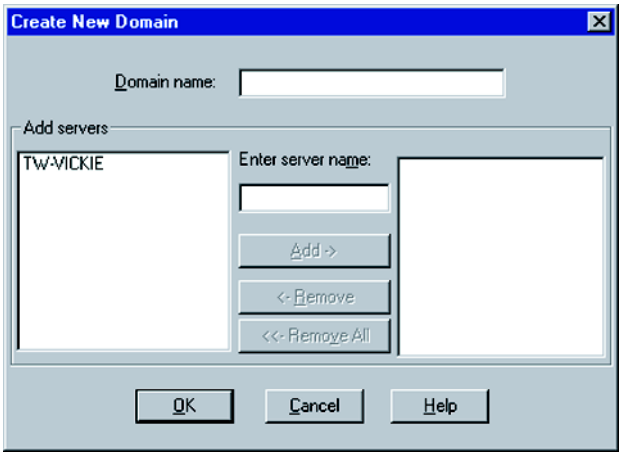


FIGURE 3-3. Create New Domain(s) window

2. Type a name in the **Domain name** text box.
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** text box.
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 window without creating a new domain.

Renaming ServerProtect Domains

A domain called **Default** is created 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** window appears.

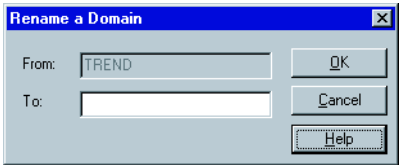


FIGURE 3-4. Rename a Domain window

3. Type the new domain name in the **To** text box and then click **OK**. Click **Cancel** to close the window 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 on your 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 3-8.

Managing Information Servers

The Information Server stores and delivers data to and from the Normal Servers. On Windows Storage Server 2003/Server 2003, 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 if 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** window appears.

2. Do one of the following:
   - Type the name or IP address of the Information Server.
   - Select the Information Server from the list.

   Click **Refresh** if you need to refresh the view of servers in the list.

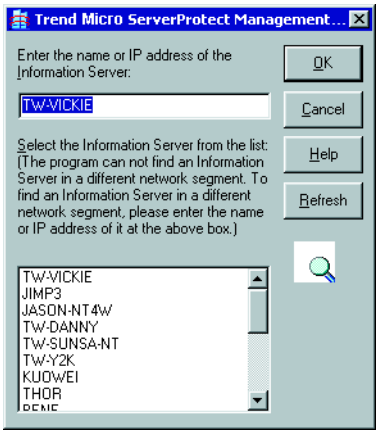


FIGURE 3-5. Trend ServerProtect Management Console window

3. Click **OK** to save your changes or click **Cancel** to close the window 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 lets you 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:

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** window appears.
2. Select the destination Information Server and click **OK**.

   A warning window appears. If you are sure you want to move the Normal Server to the selected Information Server, click **OK**.

Configuring Updates

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

Update Components

The following are the ServerProtect components that you can update:

- **Virus pattern file**: The virus pattern file is a collection of virus signatures (Database). With so many new viruses being detected each month, this is understandably the most often updated component.
- **Scan engine**: The scan engine is the software component that performs the actual virus detection function.

How Updates Work

The following figure shows how ServerProtect deals with a typical request to download and deploy updates in a ServerProtect network.

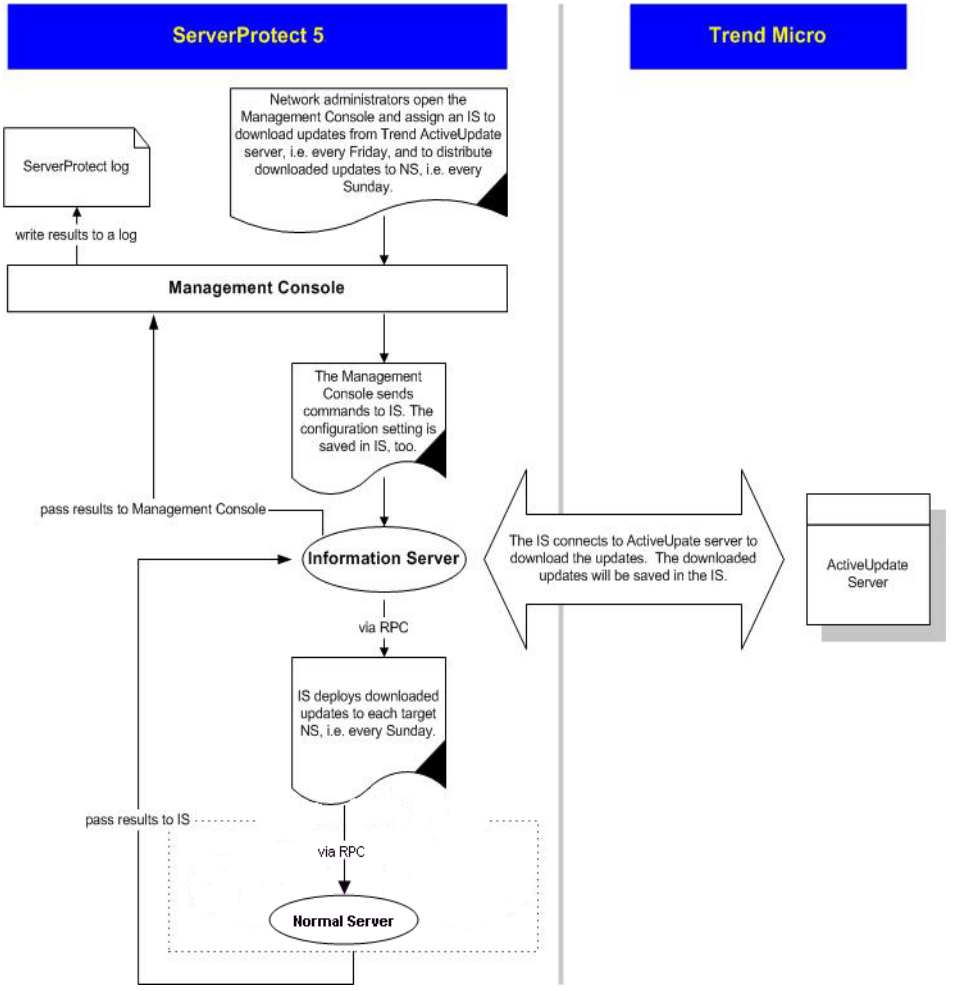


FIGURE 3-6. How Updates Work chart

Verifying the Current Version of Files

ServerProtect lets you 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.

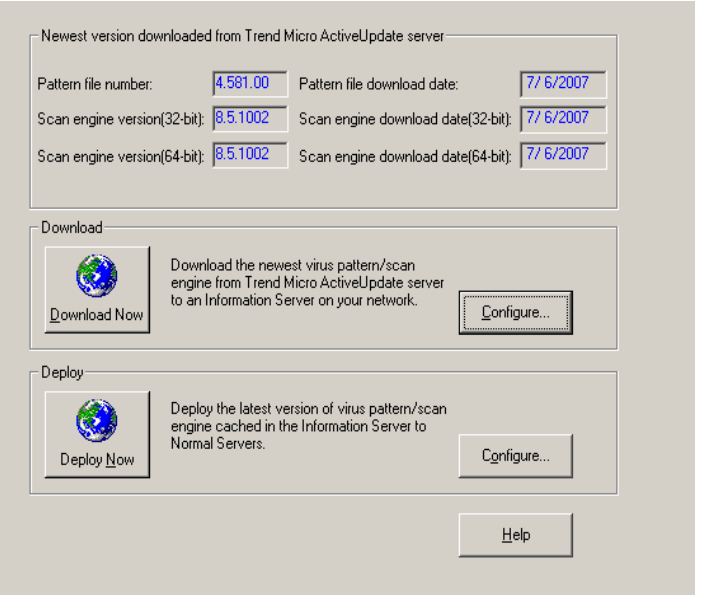


FIGURE 3-7. Trend Micro ServerProtect Update Main Screen

The version information for the virus pattern file and scan engine used by the system are shown at the top of the **Update** screen.

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** window.
3. Click **Internet** and then type the following URL to download the update files from the Trend Micro update server:

   ```
   serverprotect-t.activeupdate.trendmicro.com/activeupdate
   ```

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

   ```
   \ProgramFiles\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** window 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 `\ProgramFiles\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, may prompt an "HTTP generic failure" or "HTTP authentication failure" message when you click **Download Now**. See *Configuring Download Settings* on page 3-20.

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** window appears.
3. Click the **Schedule Setting** tab.

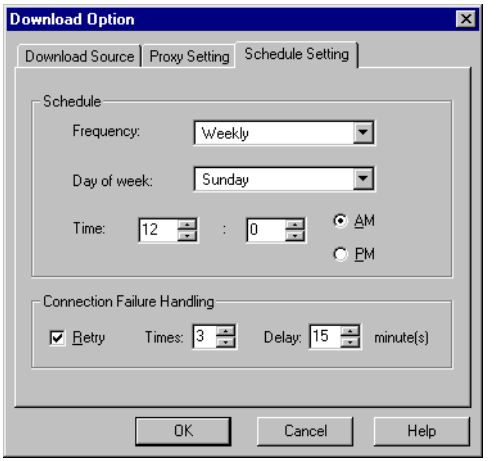


FIGURE 3-8. Download Option--Schedule Setting window

4. Under **Schedule** in the **Frequency** list, click a download frequency. You can select **None**, **Daily** or **Weekly**. If you do not want to schedule a download, click **None**. If you click **Weekly**, in the **Day of Week** list, click a day.
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 latest update files

To configure 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** window appears.

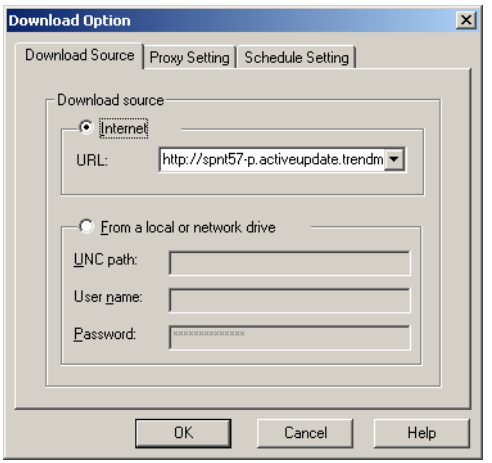


FIGURE 3-9. Download Option window

Configuring 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** window appears.

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

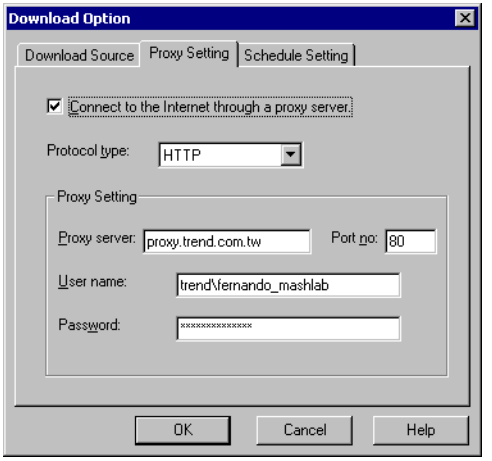


FIGURE 3-10. Download Option--Proxy Setting window

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 SOCKS 4.
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 window appears. Click **Yes** to proceed with the manual update deployment. The **Deploy** window appears.

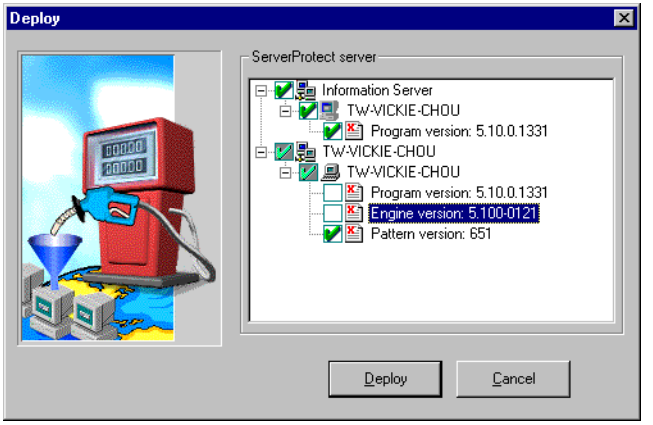


FIGURE 3-11. Deploy window

The current version of each server component is shown in a server tree. The **Pattern version** check box is selected by default.

3. Select the check box(es) of the components you want to update. To update all components in a Normal Server, select the server's check box.
4. Click **Deploy** to activate the deployment process, or click **Cancel** to discontinue.

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 3-28.

For more information on how to configure a scheduled task, refer to *Creating Tasks* on page 3-29.

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** window appears.

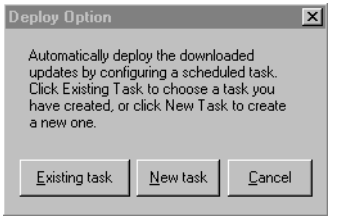


FIGURE 3-12. Deploy Options window

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 3-29 and *Modifying an Existing Task* on page 3-35 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. The virus pattern and scan engine can be rolled back. This is necessary if there is a software compatibility issue or if the update files were corrupted during the original download.

Note: If both virus pattern and scan engine files were originally deployed, you must roll both of them back.

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.

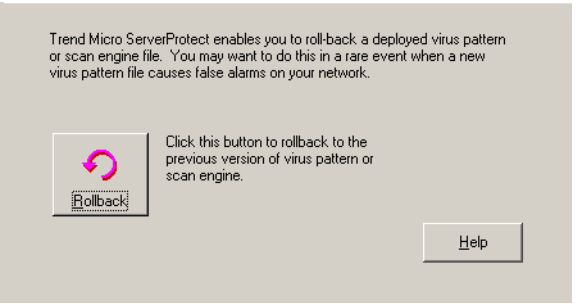


FIGURE 3-13. Roll Back Configuration window

2. Click **Rollback**. The ServerProtect **Rollback** window appears.

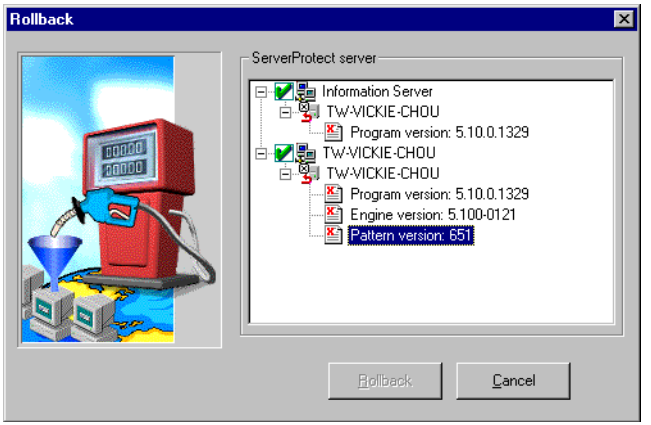


FIGURE 3-14. Rollback window

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 cannot roll back the virus pattern or scan engine past the immediately preceding version.

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**: Enable different Real-time Scan options for different tasks, for example, scanning incoming files only when network performance is normal
- **Scan Now**: Check whether your server is virus-free
- **Purge logs**: Define 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**: Export logs as CSV files for use in other applications
- **Print logs**: Choose a network printer to print logs that meet a certain criteria
- **Run statistics**: Compile and display statistics about virus scanning on your server
- **Deploy**: Define when to distribute the updates of virus pattern and scan engine components to other ServerProtect servers

FIGURE 3-15. Task Wizard window

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 can not 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** window appears.

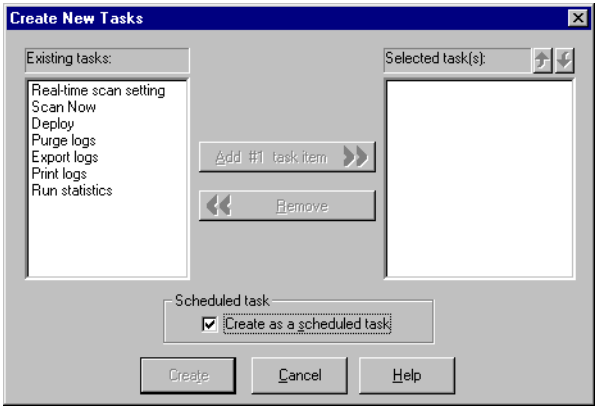


FIGURE 3-16. Create New Tasks window

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.

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.

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

Creating a Scheduled Task

Creating scheduled tasks are easy to configure and save you time.

To create a scheduled task:

1. Follow steps 1 through 6 in the *Creating Tasks* on page 3-29 section. Make sure you select the **Create as a scheduled task** check box under **Scheduled task** (see Figure 3-16). The **Task Wizard** window appears.
2. Click **Next**. The **Schedule Settings** window appears.

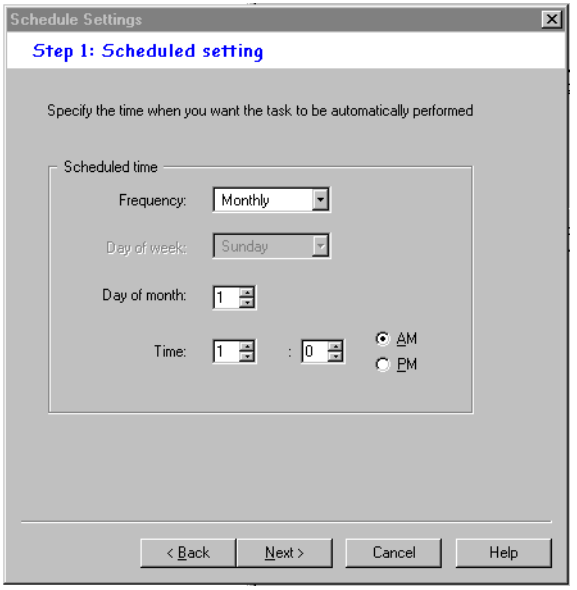


FIGURE 3-17. Schedule Settings window

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

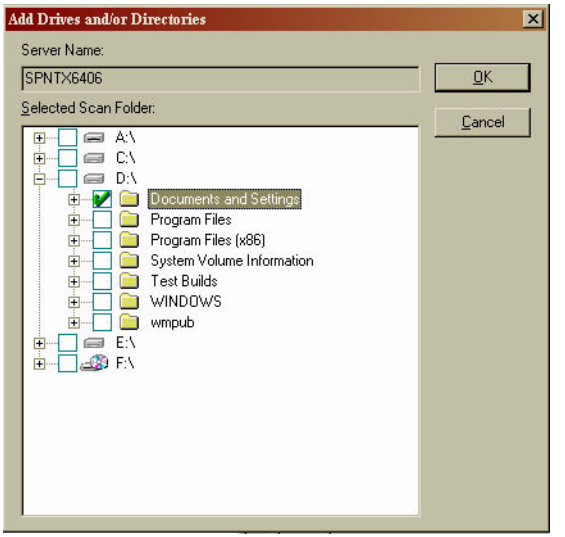


FIGURE 3-18. Add Drives and/or Directories window

Creating a Default Task

You can define a default task in the last screen of the task wizard, the **Task Information** window, 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.

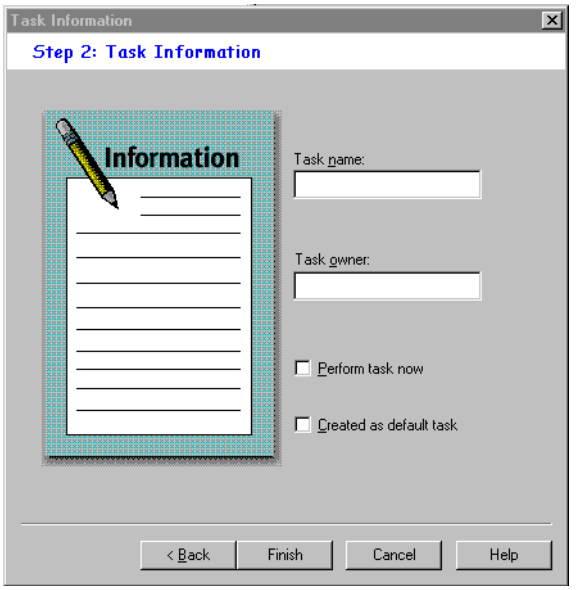


FIGURE 3-19. Task Information window

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.

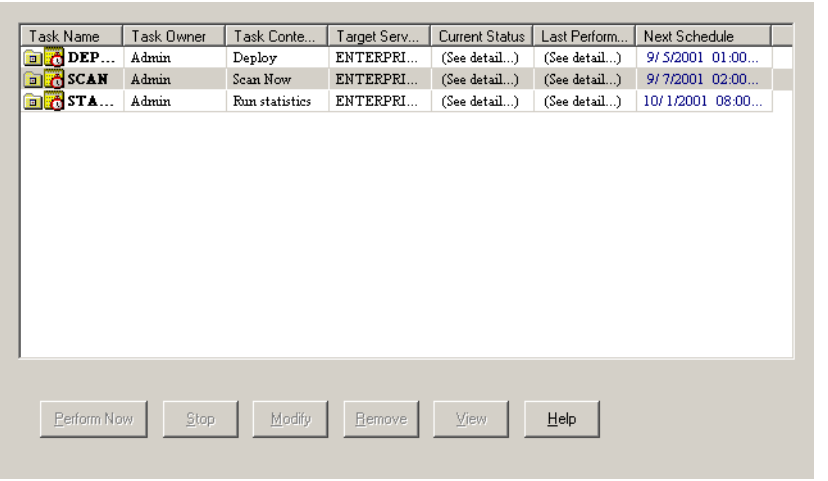


FIGURE 3-20. Viewing Existing Tasks table

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** window appears.

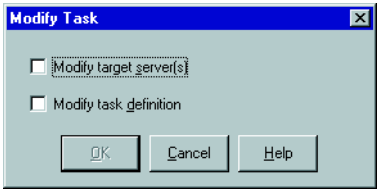


FIGURE 3-21. Modify Task window

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** window select and add the server on which you want to run the task.
2. Click **Add**.

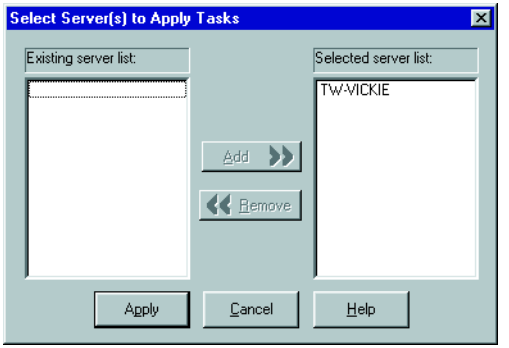


FIGURE 3-22. Select Servers to Apply Tasks window

3. Click **Apply**. To close the window 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.

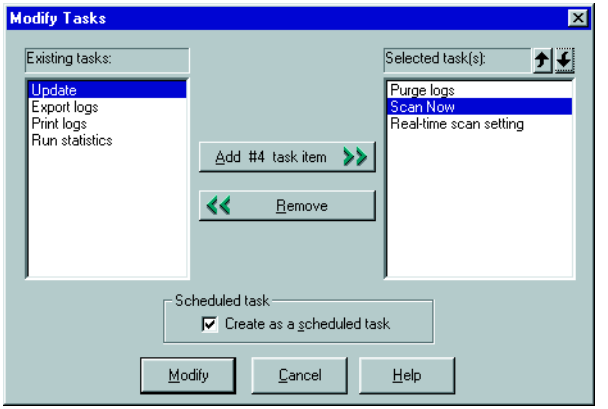


FIGURE 3-23. Modify Tasks window

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** window without saving your changes.

Viewing an Existing Task

The attributes of any existing task can be viewed from the **Existing Task** window. 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** window appears.

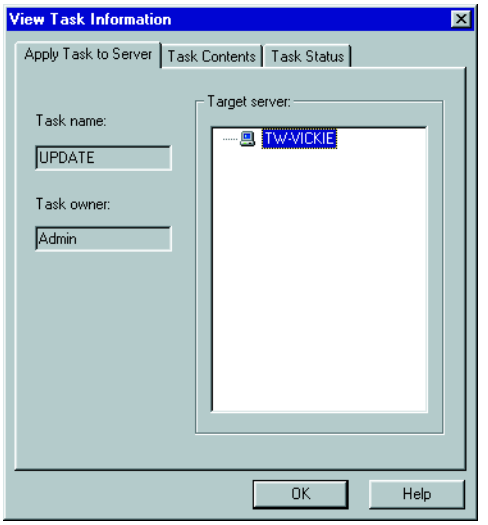


FIGURE 3-24. View Task window

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 your network that the task will run on.
- **Task Contents**: All of the functions that make up the task are displayed. Click 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 that the task will run on. 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** window.

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 3-43 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 infection**: Detection of an infected file on the server
- **Attempt to change write-protected file**: Any attempt to change the write-protected settings
- **Real-time configuration change**: Changes to the configuration settings of Real-time Scan
- **Service load/unload**: To stop/start the ServerProtect
- **Virus pattern out-of-date**: Expiration of the virus pattern file

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.

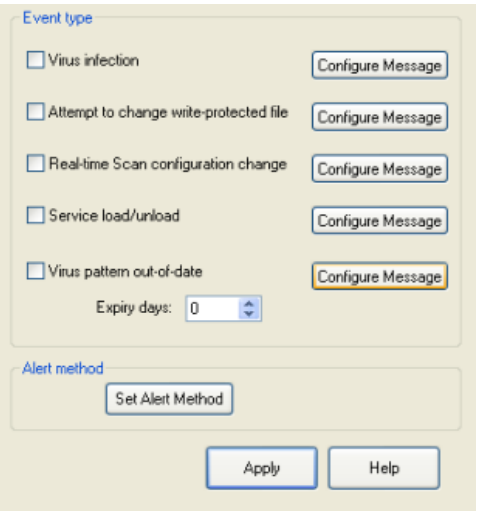


FIGURE 3-25. ServerProtect Standard Alert Configuration window

3. Select the event type check box(es).
4. Click **Configure Message** for each selected event. The **Configure Alert Message** window appears.
5. Type your desired settings, and then click **OK** to close the window.
6. Click **Set Alert Method** to select the way that you want to be notified. Refer to *Setting Alert Methods* on page 3-43 for detailed information.
7. Click **Apply** to save your changes.

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.

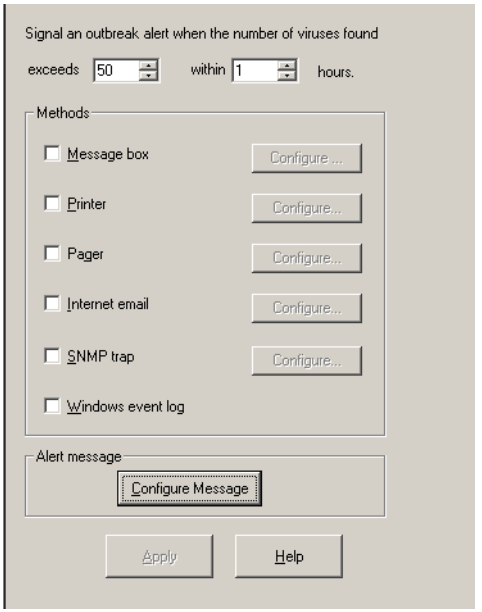


FIGURE 3-26. ServerProtect Outbreak Alert Events Configuration Window

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 notification settings for the selected methods. For detailed information about each modification method, refer to *Setting Alert Methods* on page 3-43.
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 is sent on detection of viruses.
- **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 doucument. For other forms of notification, refer to the online help.

To configure an alert to be sent via 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** window appears.

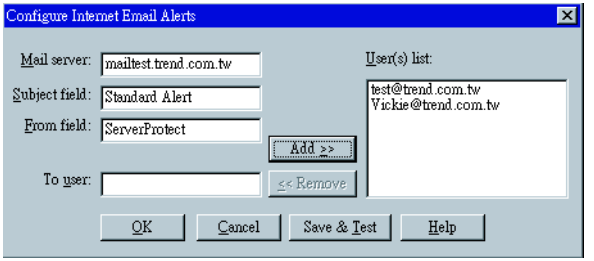


FIGURE 3-27. Configure Internet Email Alerts window

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** window.

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** window. 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.

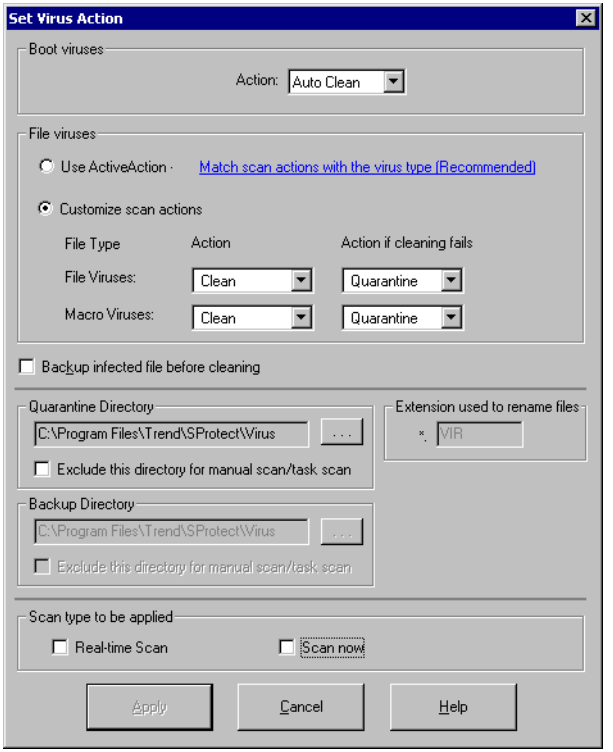


FIGURE 3-28. Set Virus Action window

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** window appears.
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.
   - 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 1-9. For more information about ActiveAction, see *IntelliScan* on page 1-16.

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 3-35.

To save a scanning profile:

1. Configure a Real-time Scan or Scan Now. See *Configuring Real-Time Scan* on page 3-49 and *Configuring Scan Now* on page 3-52.
2. Click **Save As/ Delete Profile**. The **Save/Delete Profile** window appears.

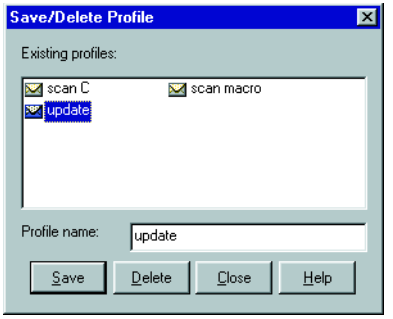


FIGURE 3-29. Save/Delete Profile window

3. Type a profile name in the **Profile name** text box.
4. Click **Save** to save the new profile. Alternatively, click **Close** to close the window 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** window 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 window 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. All incoming/outgoing files are monitored, thus infected files are prevented from being copied to or from a server.

Configuring Real-Time 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 1-16 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.

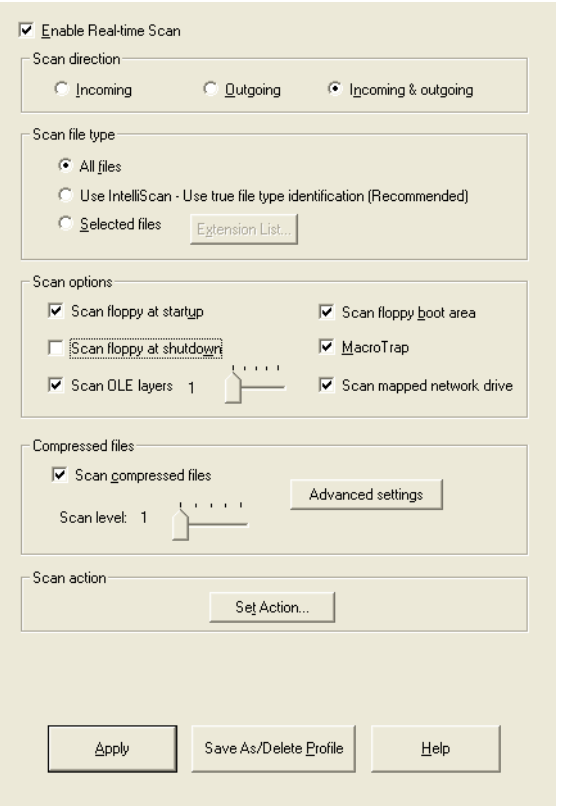


FIGURE 3-30. Real-time Scanning Configuration Window

3. Select the **Enable real-time scan** check box.
4. 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

5. 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 1-16.
   - **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 3-57.
6. 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 Real-Time Scan* on page 3-49 for additional information on each scan option.
7. 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.
8. Click **Set Action** to configure how ServerProtect acts on infected files. See *Defining Actions Against Viruses* on page 3-45.
9. 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:
   - Click **Scan Now** > **Scan Now** on the side bar.
   - Click **Do** > **Scan Now** on the main menu.

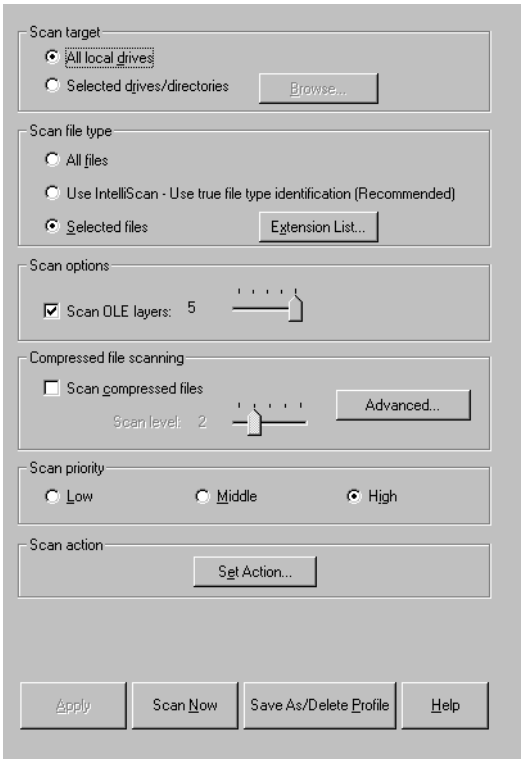


FIGURE 3-31. Scan Now Configuration window

3. 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** window appears. Select the check box(es) for the drives or directories you want to scan, then click **OK** to close the window.

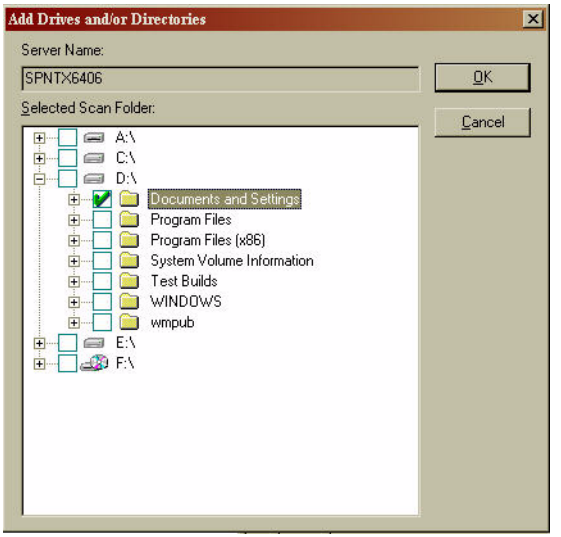


FIGURE 3-32. Add Drives and/or Directories window

4. 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 1-16.
   - **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 3-57.
5. 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.
6. 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.

7. Under **Scan priority**, click **Low**, **Middle**, or **High**. A high scan priority consumes more CPU resources, but can complete scan jobs faster.
8. Click **Set Action** to configure how ServerProtect acts on infected files. See *Defining Actions Against Viruses* on page 3-45.
9. Click **Apply** to save your changes or click **Save As Profile** to recall your configuration settings at a later time.

Running the Scan Now Tool on Windows Normal Servers

Use the Scan Now tool to scan Windows Storage Server 2003/Server 2003 servers 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** window 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** window 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 3-29 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 add 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** window then appears.

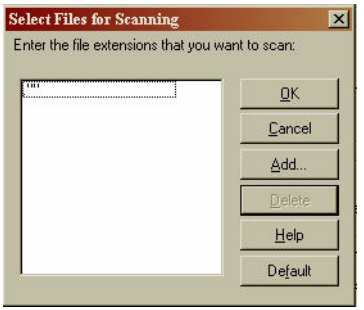


FIGURE 3-33. Select Files for Scanning window

2. Do one of the following:

   - Click **Add**. The **Add Program File Extension** window appears.

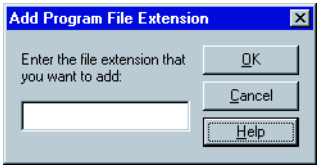


FIGURE 3-34. Add Program File Extension window

Type the file extension that you want to add in the text box, and then click **OK** to add the extension to your list. Alternatively, click **Cancel** to close the window without saving your changes. Finally, click **OK** to close the **Select files for Scanning** window.

- Click **Default** to add all the default file extensions and then click **OK** to close the **Select files for Scanning** window. 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**.

Chapter 4

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?
- Installing and Removing the Control Manager Agent for ServerProtect
- Control Manager Agent for ServerProtect Features
- Outbreak Prevention Services

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/ControlManager
   ```

   Where computer name is the IP address or host name of the Control Manager server. The Control Manager console appears.

2. In **User ID** and **Password**, type a user ID and password. The User ID must have access privileges for the Control Manager console and can be an Operator, Power User, or Administrator.
3. Click **Products** on the menu.
4. Click **Add/Remove Product Agents** on the left-hand menu.
5. Right-click the **public encryption key** link, then select **Save 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 Server 2003/Server 2003 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 Website 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 (Scan Now).
- Enable a Real-time Scan.
- Deploy a virus pattern file.
- Deploy a scan engine file.

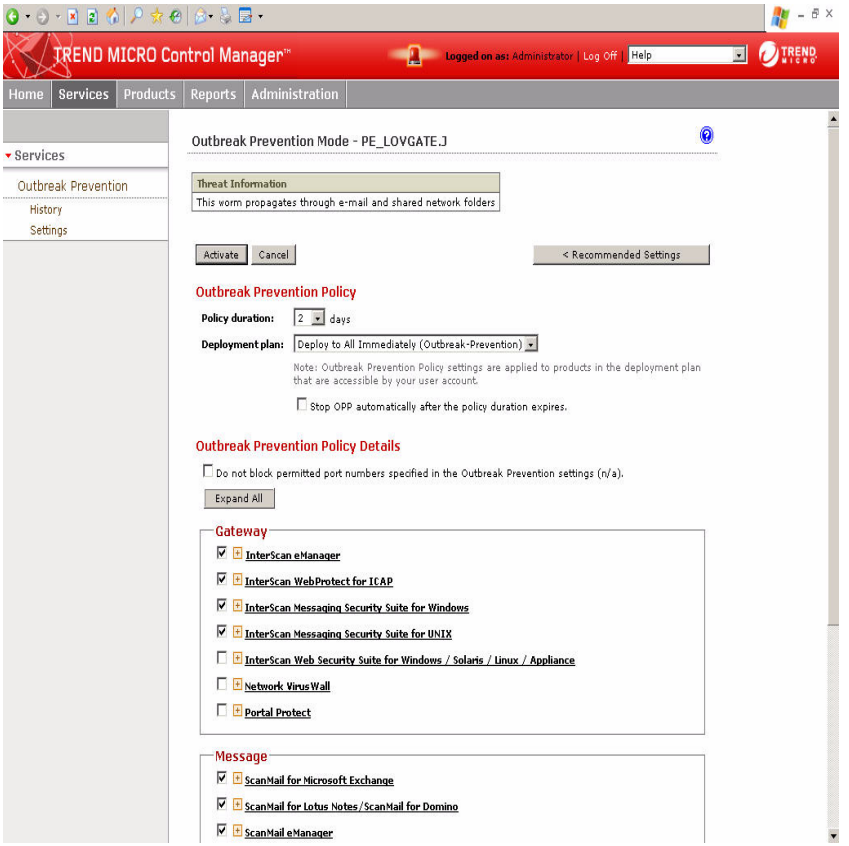


FIGURE 4-1. Services screen

The Services screen is your primary interface with the Trend Micro Outbreak Prevention Service, and is the principal means of implementing outbreak prevention policies.

Outbreak Prevention Policy (OPP)

Outbreak Prevention Policy (OPP) is a collection of settings that you can apply to ServerProtect using Outbreak Commander. These settings are created by Trend Micro in response to virus outbreaks, and provided to Control Manager users as part of the Outbreak Prevention Service.

These settings are specifically designed to protect your network against the cause of the outbreak, and are only provided for relevant products. For example, viruses that only propagate through email will only have policies with settings for messaging systems.

Chapter 5

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
- Trend Micro Security Information
- Registering Trend Micro ServerProtect
- Using Knowledge Base
- Sending Trend Micro Your Viruses
- TrendLabs

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 Website.

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 Website:

`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 Website:

`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** window 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

Converting the ServerProtect Trial Version

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
- Viewing the Serial Number List
- Updating a Serial Number

The Software Evaluation Period Window

If you install the trial version of ServerProtect, the **Software Evaluation Period** window appears every time you open the Management Console. The **Software Evaluation Period** window shows which Normal Servers are using the trial version and the number of days remaining until they expire.

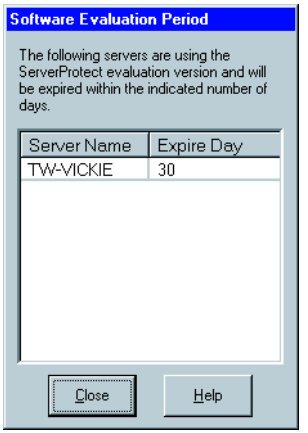


FIGURE A-1. Software Evaluation Period window

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** window appears.

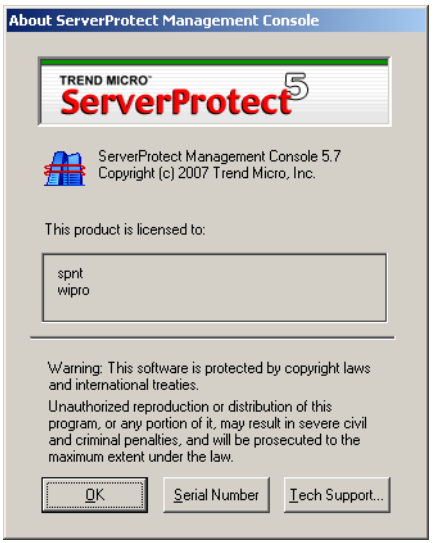


FIGURE A-2. About ServerProtect Management Console window

2. Click **Serial Number**. The **Serial Number List** window appears showing you all the ServerProtect Normal Servers on your network, along with their respective serial numbers.

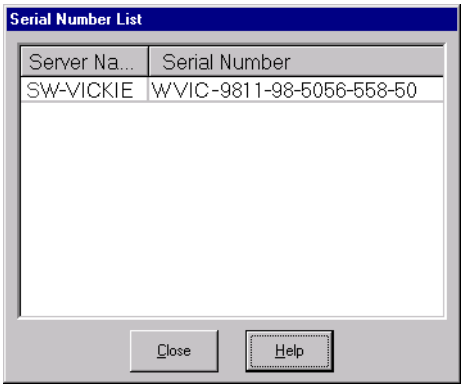


FIGURE A-3. ServerProtect Serial Number List Window

3. Click **Close** to close the **Serial Number List** window, and then click **OK** to close the **About ServerProtect Management Console** window.

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** window appears.

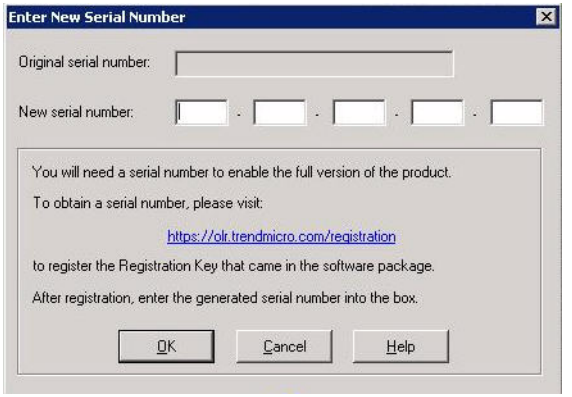


FIGURE A-4. Enter New Serial Number window

3. Type the new serial number in the **New serial number** text boxes.
4. Click **OK**. Otherwise, click **Cancel** to close the window.

Index