Chapter 5: Configuring ServerProtect

Chapter Objectives

After completing this chapter, you should be able to achieve the following objectives:

- Describe the types of ServerProtect tasks
- Describe which actions can be taken on infected files
- Describe which other task-related parameters can be set
- Explain how to configure notifications

Configuring and Performing Tasks

Tasks automate routine procedures, thereby improving antivirus management efficiency and increasing control over antivirus policies. ServerProtect enables you to create your own tasks so that your Normal Servers can perform multiple functions simultaneously.

Understanding Task Icons

The task icon—which appears next to every task in the Existing Tasks list—offers visual information about the nature of a task. Figure 5-1 illustrates the meaning of the task icons:

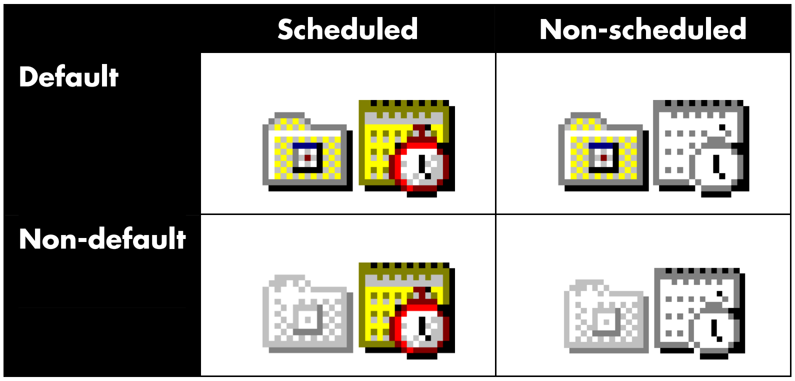


Figure 5-1: Task icons

Default Tasks

ServerProtect automatically creates default tasks whenever a Normal Server is installed. When you install ServerProtect for the first time, you immediately have three default tasks: Scan, Statistics, and Deploy. These tasks can be edited to suit your needs, but you cannot change the task name, the owner, and its default status.

You can also create new default tasks. By creating new default tasks, you eliminate the need to recreate frequently executed tasks on each new Normal Server.

Scheduled Tasks

Using the ServerProtect Task Wizard (described below), you can schedule tasks that ServerProtect performs automatically at user-configurable intervals.

ServerProtect Task Wizard

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

Real-Time Scan Setting You can use this function to scan all files as they are accessed. You can also use this function to design several real-time scans. For example, you can create a real-time scan that scans incoming files only when network performance is normal.

Scan Now You can use this function to perform a manual scan.

Purge Logs You can use this function to define which types of logs should be purged from the database. You can enable automatic purging of virus logs that are older than a preset age.

Export Logs You can use this function to export logs as comma-separated value files for use in other applications.

Print Logs You can use this function to choose a network printer to print logs according to selected criteria.

Run Statistics You can use this function to compile and display statistics about virus scanning on your server.

Deploy You can use this function to specify when the server will distribute the updates of virus pattern, scan engine, or program components to other ServerProtect servers. For example, you can choose to distribute virus pattern and scan engine updates every week (Task A) and distribute program files every month (Task B). If you schedule updates, you do not need to remember to distribute updates. Scheduled updates help ensure that your servers are not at risk because your antivirus program is outdated.

✔ **Note:** *When you arrange the sequence of functions in a task, you must put the Deploy function last. Otherwise, the task cannot be performed successfully.*

Lab Exercise 2: Using the ServerProtect Task Wizard

Configuring Virus Scanning

When ServerProtect scans a file for viruses, it compares the file against the virus-pattern file, which contains the signatures of known viruses. This process is typically a resource-intensive process. Although scanning every file that is transferred or modified on your server is the safest option, it might reduce server performance.

Because today's networks are complex, ServerProtect provides a variety of configuration options. You can use these options to customize virus scanning for your company's unique network environment.

Considerations

Before you begin to configure virus scanning for your network, you should evaluate how each server is used. By gathering detailed information about your servers, you can configure virus scanning to protect the server and minimize the impact of virus scanning on the server's resources.

You should gather information such as the following:

- How frequently is the server is accessed? Are some directories accessed more frequently than others?
- What is the CPU utilization on the server? How much RAM are other services using?
- What type of server is it (database server, file server, management server, application server, or archive server)?
- How many users access the server?
- Are any users accessing the server remotely? If so, what type of connection are they using?
- What types of files are stored on the server? For example, are the files encrypted, password-protected, graphic files, files that contain macros, compressed files, or Java archive (JAR) files?
- What are the possible entry points for viruses?
- What peripherals are attached to the server? How frequently are these peripherals accessed?
- Is performance an issue for users? For example, have any users complained that they have to wait for files to open or to be saved?
- What other services are running on the server, and how resource-intensive are those services?

If you do not have a management program that provides all of this information, you might be able to gather some of the information from users. You could send users a short survey that asks them questions such as what type of files they are using and how often they access files on a particular server.

In addition to using the information you gather to configure virus scanning, you can also use the information to educate users and your upper management. You can present the information to upper management and explain the choices that you have made to protect the network.

Scan Types

To provide virus protection for complex network environments, ServerProtect includes three types of virus scanning:

Manual Scanning (Scan Now)	Invokes an immediate virus scan that runs once and stops
Real-Time Scanning	Runs continually on the server
Scheduled Scanning	Runs periodically

Manual Scanning

When you run manual scanning, ServerProtect checks every file that you configure ServerProtect to check. Manual scanning is an effective way to check a server that has not been scanned recently or that you suspect might have been exposed to a virus.

You can launch a manual scan in either of the following ways:

- From the Management Console
- From the Normal Server

To run a manual scan from the Management Console, select the Scan Now bar from the sidebar. To run a manual scan from the Normal Server, access Windows Explorer, locate **ScanNow.exe** and double-click it. (The default location of **ScanNow.exe** is ***C:\Program Files\Trend\SProtect***.)

ServerProtect performs the manual scan according to the configurations set by the Management Console. For example, you can configure parameters such as the type of file to be scanned or directories that should not be scanned.

Real-time Scanning

When you enable real-time scanning, ServerProtect monitors all file I/O events on the Normal Server. If a user accesses a file on the server, ServerProtect scans the file to ensure that it is not infected. Real-time scanning prevents users from copying infected files to or from the server. Files on the server or any other storage media will neither infect nor be infected.

Trend Micro recommends that you enable real-time scanning on servers that are frequently used. Because users frequently copy files to and from these servers, they are at higher risk for virus infections. Real-time scanning helps ensure that your company's data is protected.

Because real-time scanning runs continually in the background, however, it is resource intensive. Depending on the server's workload, real-time scanning can affect server performance. Using the information you gathered about the server, you can weigh the benefits of real-time scanning against the possibility of performance issues. You can also determine which directories and files are at the highest risk for virus infections and enable real-time scanning only for those directories and files. You can then run a scheduled scan during low usage times to check all directories and files for virus infections.

Scheduled Scanning

When you configure a scheduled scan, it runs only at the specified time on the servers that you select. Scheduled scanning is an effective way to check infrequently used servers. Because scheduled scanning can be performed after business hours, you can use this type of scanning to conserve server resources during peak usage.

To configure scheduled scanning, you create a scheduled task. (For more information about ServerProtect tasks, see the preceding section.) Each ServerProtect server includes a Default Scan task, which scans all of the local directories for viruses every Friday. You can modify this task or create a new one if the current default setting does not suit your needs.

Configuring Scanning Parameters

ServerProtect provides flexibility in how the files on your network servers are scanned. You can configure the following parameters:

Scan direction Configure this parameter to scan files that are copied to the server, from the server, or both. This parameter is not available for manual scanning.

Scan file type Configure this parameter to control which file types are scanned and which are not.

Scan options Configure this parameter to optionally scan the server's floppy disk drive during startup or shutdown or to scan the computer's hard-disk-drive boot sector.

Compressed files Configure this parameter to scan compressed archive files (such as ZIP or CAB) and to control how many layers should be expanded during scanning.

Scan action Configure this parameter to specify which actions to take against file, boot-sector, and macro viruses. You also configure this parameter to configure the directory where ServerProtect saves infected files and backup files.

Scan target Configure this parameter to specify which drives should be scanned. This parameter is not available for real-time scanning.

Scan priority Configure this parameter to specify the scanning priority of the server.

Scan Direction

You can determine which I/O activities ServerProtect monitors—incoming files, outgoing files, or both incoming and outgoing files. For example, you might determine that there is little or no risk that files being copied from the server are infected with viruses. In this case, you would configure ServerProtect to monitor only incoming files.

Scan File Types

You can specify which types of files ServerProtect should scan for viruses. Because only certain types of files can contain viruses, you can use this parameter to scan only those files that might harbor a virus.

Scan Options

You can configure ServerProtect to monitor the server's floppy diskette drive and floppy boot area, which historically have been vulnerable to viruses. You can configure ServerProtect to scan the floppy diskette drive at startup and at shutdown.

You can use the Network Trap Tool to create a Bait folder that contains files that viruses are likely to infect. Certain viruses—such as the PE.FunLove.4099 virus—actively seek out shared folders to infect as many connected users as possible. The Network Trap tool automatically copies the contents of the Bait folder to a newly created shared folder. When a virus infects the files in the Bait folder, the new virus notification feature alerts you of the infection before it can spread to the rest of the network.

Scan Compressed Files

You can configure ServerProtect to scan compressed files, and you can also configure the number of layers—up to five—that ServerProtect scans. If ServerProtect detects that a compressed file is virus-infected, it records the file name of the first layer in a log file. When you view the log file, you can take action against the infected file. For example, you can rename, delete, or remove the file.

ServerProtect can clean the first layer of infected ZIP files. To clean other types of compressed files or to clean other layers of ZIP files, you must manually decompress the files and perform a manual scan on them.

Actions Against Infected Files (Set Virus Actions)

You can configure the kinds of actions ServerProtect takes against infected files. You can also configure different actions for boot viruses, file viruses, and macro viruses. The ServerProtect virus-cleaning engine can take the following actions against an infected file:

Bypass/ Ignore If you select this action, ServerProtect skips over the file in a manual scan without taking any corrective action. However, ServerProtect still records the detection of the virus in the log. In a real-time scan, ServerProtect treats the file as deny write, which prevents it from being copied or modified.

Delete If you select this action, ServerProtect deletes the infected file.

Rename If you select this action, ServerProtect renames the infected file by changing the file extension to VIR. Changing the file extension prevents the file from being executed or opened. If a file with that name and the VIR extension already exists, the file will be renamed VI1, VI2, and so on until V99.

Move If you select this action, ServerProtect moves the infected file to a designated folder. If you want to move infected files to a directory of your choice, you must use the **Browse** button to specify a drive on the server. In addition, you can change the file extension of the moved file to prevent it from being inadvertently opened or executed.

Clean If you select this action, ServerProtect attempts to clean the virus code from the file. Because the cleaning process sometimes corrupts the file and makes it unusable, you should make a backup copy of the file before cleaning. You choose the backup directory by clicking the **Browse** button at the bottom of the *Set Virus Action* screen and selecting a local directory.

✔ *Note: If you select Clean as the antivirus action, you can specify a secondary action if the cleaning process fails.*

In addition to configuring actions against viruses, you can configure the following:

- Location of the quarantine area for infected files
- Extension of infected files that are renamed
- Backups of infected files and the location where backups are stored
- Type of scan that is associated with the settings you select

Scan Target

If you are configuring a manual scan, you can select the drives and directories that are scanned. You can choose one of the following options:

Scan all local drives Provides the maximum protection but uses more server resources.

Scan selected drives or directories Targets specific drives or directories. Select this option to check directories that are especially vulnerable to virus protection. You might also want to select this option if performance is an issue. If you limit the scan to certain drives, fewer server resources will be used.

Scan Priority

You select one of the following options to configure the priority for scanning:

Low Use this option when the risk of infection is low and performance is a high priority.

Medium Use this option to maintain a balance between performance and protection.

High Use this option when the risk of infection is highest, when finding a suspected virus is of greater importance than maintaining high performance.

Scanning Profiles

You can create scanning profiles to avoid repeatedly reconfiguring scans. When you configure a real-time or manual scan, you can click the **Save/Delete Profile** button to save those configuration options. The next time you create a scheduled scan task, you can either choose an existing profile or configure new scan options.

Configuring the Exclusion List

You can configure ServerProtect to exclude selected directories and files from virus scanning. You can use the exclusion list in the following ways:

- If the ServerProtect scan engine is incorrectly detecting malware in files that are not infected, you can temporarily include the files in the exclusion list.
- If you quarantine infected files in one directory, you should include this directory in the exclusion list so that ServerProtect does not continually scan the quarantined files.

- If performance is an issue, you can exclude files that are resource intensive to scan. For example, scanning JAR files is extremely resource intensive. You might want to exclude these files from real-time scanning and use scheduled scanning to check them after business hours. Of course, you must evaluate the risk of virus infection from this type of file (or any type of file) before you exclude those files from real-time scanning.

You can configure two kinds of exclusion lists in ServerProtect:

Excluded directory list	Exclude specified directories from being scanned
Excluded file list	Exclude specified files from being scanned

Configuring the Deny Write List

ServerProtect provides an additional level of protection beyond file checking. By using the Deny Write list, you can prevent users from modifying or deleting selected directories or files, and you can specify which file extensions are protected.

Users who have Supervisor or equivalent privileges are also blocked from making modifications to protected file types in any directory. This blockade prevents supervisor-equivalent users from unknowingly spreading viruses to areas where only they have modify rights. Viruses that infect these files can spread quickly.

To prevent a particular user from modifying files in the selected directories, you designate that user as a restricted user. If necessary, you can also grant a user temporary modify rights that expire after a specified time has passed.

Adding Drives or Directories to the Deny Write List

When a server drive or directory is on the Deny Write list, the directory and the files within it that you specify have the read-only attribute. When you include a directory in the Deny Write list, viruses cannot save data to that directory. You might want to include directories such as the public user directories in the Deny Write list.

Information for a NetWare Environment

If you manage NetWare servers, you can configure some additional parameters for virus scanning. For example, when you configure the Deny Write list, you can prevent selected users from modifying or deleting protected directories and files. You can also specify certain directories and files to be exempted in the Deny Write list.

Granting Temporary Modify Rights to a User

If a user needs to update a program or make changes to protected files or directories, you can give time-limited modify rights to that user. The user who is granted these rights cannot be on the Restricted Users list.

Restricting Modify Rights for Selected Users

In addition to designating deny write folders, you can have more control over the network by restricting who has modify rights to network files.

When you are configuring the Exclusion list for a NetWare server, you configure who can have temporary access rights to a folder or a file. The file or directory in the Exclusion list will not be scanned during a scanning task.

In addition, you can configure scanning for Macintosh files that are stored on a NetWare server. You can specify that ServerProtect should skip Macintosh files, scan only Macintosh application files, or scan Macintosh files that have resource forks.

Configuring Notifications

Antivirus software is almost useless if it locates viruses but never alerts a user or an administrator that a virus has been found. For this reason, you can configure notifications that are generated in response to virus events. Whenever a virus infects a computer on your network, you are notified of the event.

You can also specify where ServerProtect sends the notifications. For example, if a server suffers a suspicious virus infection, you can configure ServerProtect to send notifications to all of the system administrators. You can also configure ServerProtect so that system administrators receive virus alerts only on the servers for which they are responsible.

Notifications are categorized into two types:

- Standard alert
- Outbreak alert

Standard Alert

A standard alert is generated whenever a fault condition that you specify is detected on a designated server. ServerProtect sends one email alert for each virus that it finds. In this way, ServerProtect eliminates sending multiple alerts, which greatly reduces the number of notifications sent for each manual scan.

Notification Events

You can configure ServerProtect to notify you when one of the following events occurs in a server on your ServerProtect network.

Virus Infection ServerProtect detects an infected file on the server.

Attempt to Modify Write-Protected File ServerProtect detects an attempt to modify a file that is protected by a deny write rule.

Real-Time Configuration Change Someone changes the configuration settings of your ServerProtect installation.

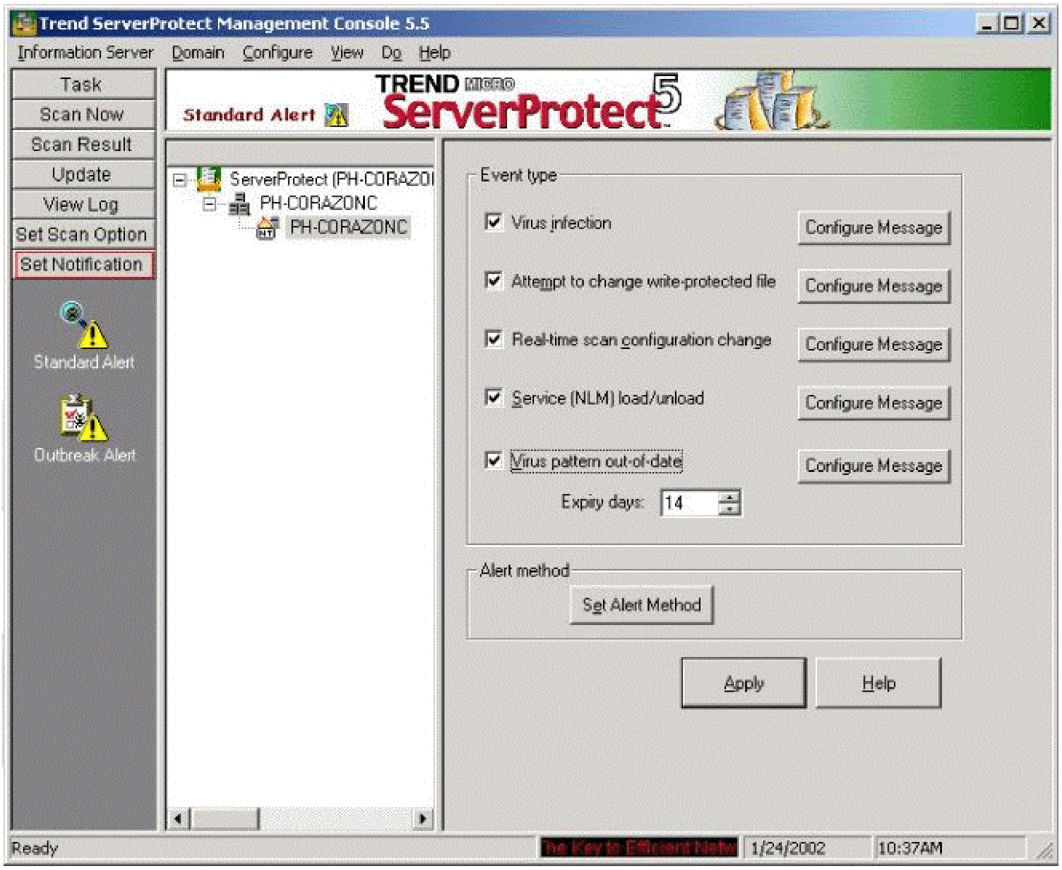
Service Unload/NLM Unload The ServerProtect Windows NT/2000 service or the ServerProtect NetWare Loadable Module (NLM) is stopped.

Virus Pattern Out-of-Date The number of days since the virus pattern file was updated is higher than the number of days you specified in the standard alert settings.

Configuring Alert Messages

You can configure the message ServerProtect sends when it detects a notification event. To configure the message, you access the *Standard Alerts* configuration window and click **Configure Messages** on the right of the event type(s) that you have selected (see Figure 5-2). When the *Configure Alert Message* dialog box appears, you can select the message parameters.

The following sections describe how you can configure alert messages for each notification event.



Event type

☑ Virus infection

☑ Attempt to change write-protected file

☑ Real-time scan configuration change

☑ Service (NLM) load/unload

☑ Virus pattern out-of-date

Expiry days: 14

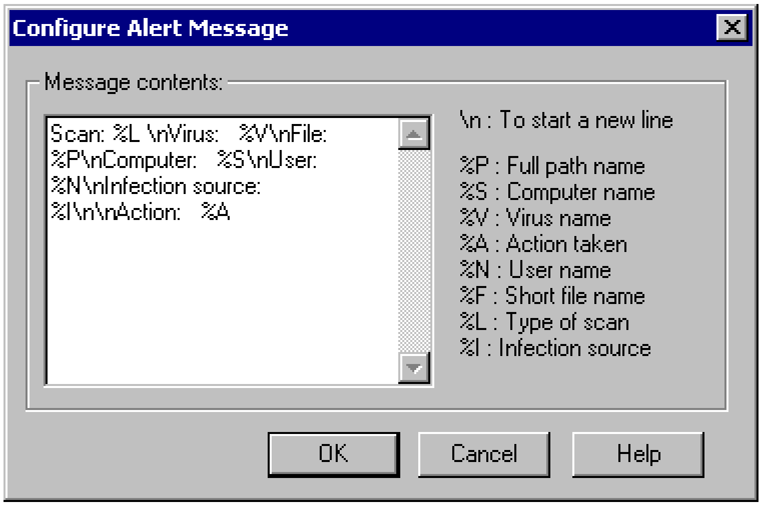
Alert method

Figure 5-2: Standard Alert configuration window

Virus Infection

To generate message text that notifies you of a virus infection on your network, you use the following special characters to display fields (see Figure 5-3). You can enter your own text to include special information about the virus infection.

- `\n` : start a new line
- `%P` : full name and path of the infected file
- `%S` : computer name where the infected file was detected
- `%V` : virus name
- `%A` : action taken against the infected file
- `%N` : user name of the person who was copying the infected file to or from the server
- `%F` : short file name of the infected file
- `%L` : type of scan that detected the infected file



Message contents:

```
Scan: %L \nVirus:   %V\nFile:
%P\nComputer:   %S\nUser:
%N\nInfection source:
%I\n\nAction:   %A
```

\n : To start a new line

%P : Full path name
%S : Computer name
%V : Virus name
%A : Action taken
%N : User name
%F : Short file name
%L : Type of scan
%I : Infection source

Figure 5-3: Configure Alert Message dialog box

ServerProtect sets the following default characters:

```
Scan: %L \nVirus: %V\nFile: %P\nComputer: %S\nUser: %N\nAction:
%A
```

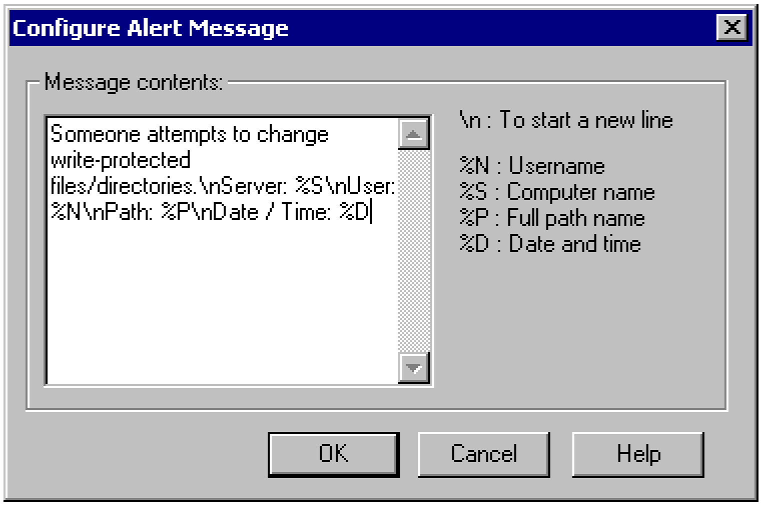
If you keep the default characters, ServerProtect sends a message that includes information similar to the following:

```
Scan: real-time

Virus: melissa

File: C:\general\letter.doc

Computer: tw-sun

User: Smith

Action: Clean, Remove
```

Attempts to Change Write-Protected Files or Directories

To generate message text that notifies you of an attempt to change write-protected files or directories, you use the following special characters to display fields (see Figure 5-4). You can enter your own text to include special information about the change attempt.

- `\n` : start a new line
- `%P` : full path name of the write-protected files/directories
- `%S` : name of computer where the write-protected files/directories reside
- `%N` : user name of the person who was copying the infected file to or from the server
- `%D` : date and time of the attempt to modify the integrity shield



```
Someone attempts to change
write-protected
files/directories.\nServer: %S\nUser:
%N\nPath: %P\nDate / Time: %D
```

\n : To start a new line

%N : Username
%S : Computer name
%P : Full path name
%D : Date and time

Figure 5-4: Configure Alert Message dialog box

ServerProtect sets the following default characters:

```
Someone attempted to change write-protected
files/directories.\nServer: %S\nUser: %N\nPath: %P\nDate/Time:
%D
```

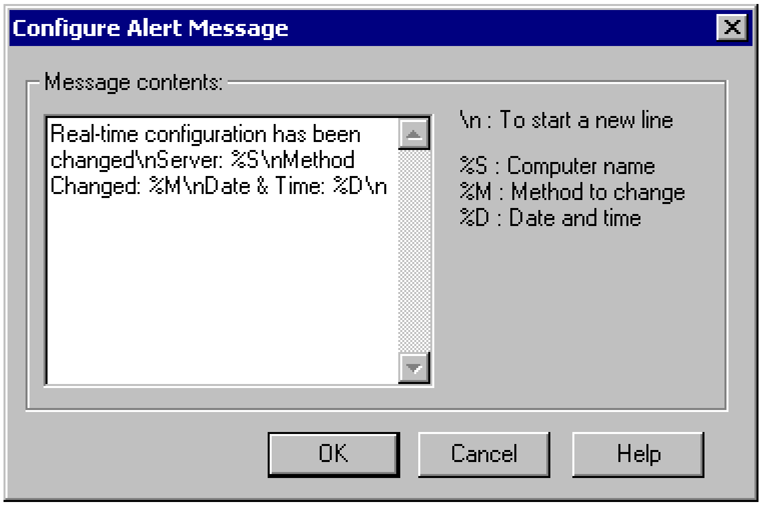
If you keep the default characters, ServerProtect sends a message that includes information similar to the following:

```
Someone attempted to change write-protected files/directories.

Server: tw-sun

User: Smith

Path: C:\generate\letter.doc

Date/Time: January 24, 12:04
```

Real-Time Scan Configuration Change

To generate message text that notifies you when there is an attempt to change ServerProtect's real-time configuration settings, you use the following special characters to display fields (see Figure 5-5). You can enter your own text to include special information about the change attempt.

- `\n` : start a new line
- `%S` : name of computer where configuration setting is applied
- `%M` : the method used to modify ServerProtect's configuration settings
- `%D` : date and time of the attempt to modify the configuration



Real-time configuration has been changed\nServer: %S\nMethod Changed: %M\nDate & Time: %D\n

\n : To start a new line

%S : Computer name
%M : Method to change
%D : Date and time

Figure 5-5: Configure Alert Message dialog box

ServerProtect sets the following default characters:

```
Real-time configuration has been changed\nServer: %S\nMethod
Change: %M\nDate & Time: %D
```

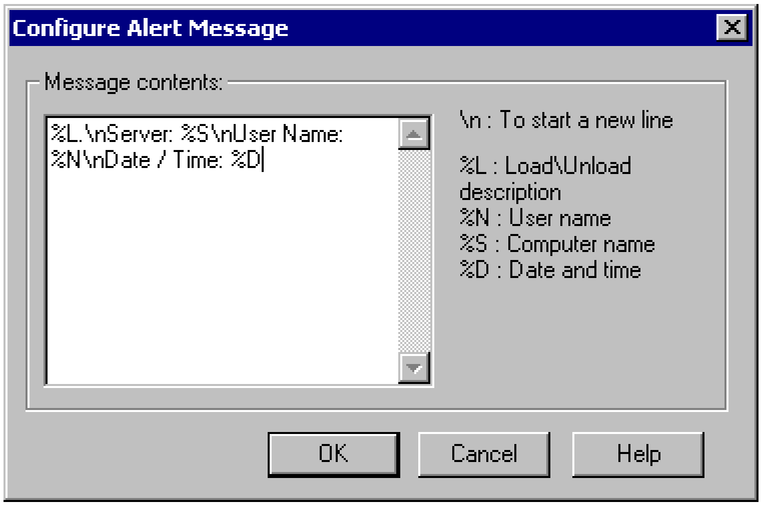
If you keep the default characters, ServerProtect sends a message that includes information similar to the following:

```
Real-time configuration has been changed

Server: tw-sun

Method Changed: compressed files

Path: C:\generate\letter.doc

Date and Time: January 24, 12:04
```

ServerProtect Service/NLM Load and Unload

To generate message text that notifies you when the ServerProtect service or the ServerProtect NLM is loaded or unloaded, you use the following special characters to display fields (see Figure 5-6). (NLM is software that runs on a NetWare server.) You enter your own text to include special information about the load or unload attempt.

- `\n` : start a new line
- `%L` : the action taken, either load or unload
- `%N` : the user name of the person who tried to load or unload the service or NLM
- `%S` : the name of the computer where a service or NLM was loaded or unloaded
- `%D` : date and time when the loading or unloading occurred



Configure Alert Message

Message contents:

```
%L.\nServer: %S\nUser Name:
%N\nDate / Time: %D
```

\n : To start a new line

%L : Load\Unload description
%N : User name
%S : Computer name
%D : Date and time

Figure 5-6: Configure Alert Message dialog box

ServerProtect sets the following default characters:

```
%L \nServer: %S\nUser Name: %N\nDate/Time: %D
```

If you keep the default characters, ServerProtect sends a message that includes information similar to the following:

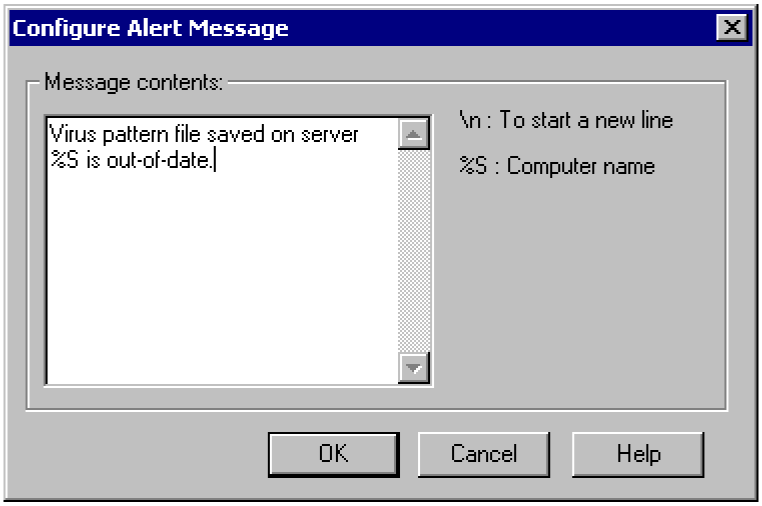
```
Service of NLM is loaded!!!

Server: tw-sun

User Name: Smith

Date/Time: January 24, 12:04
```

Virus Pattern Out-of-Date

To generate message text that notifies you when the virus pattern file is out-of-date, you use the following special characters to display fields (see Figure 5-7). You can enter your own text to include special information about the virus pattern file expiry.

✔ ***Note:*** *When determining if the virus pattern is out-of-date, ServerProtect compares the current system date with a creation date hidden within the virus pattern file. This date is not visible. When the difference between the system date and this hidden date is more than the number of days you specified in the standard alert settings, the alert message is triggered.*

- `\n` : start a new line
- `%S` : the name of servers where virus pattern files are saved


Configure Alert Message

Message contents:

```
Virus pattern file saved on server
%S is out-of-date.
```

Figure 5-7: Configure Alert Message dialog box

Server Protect sets the following default characters:

```
Virus pattern on server %S is out-of-date.
```

If you keep the default characters, ServerProtect sends a message that includes information similar to the following:

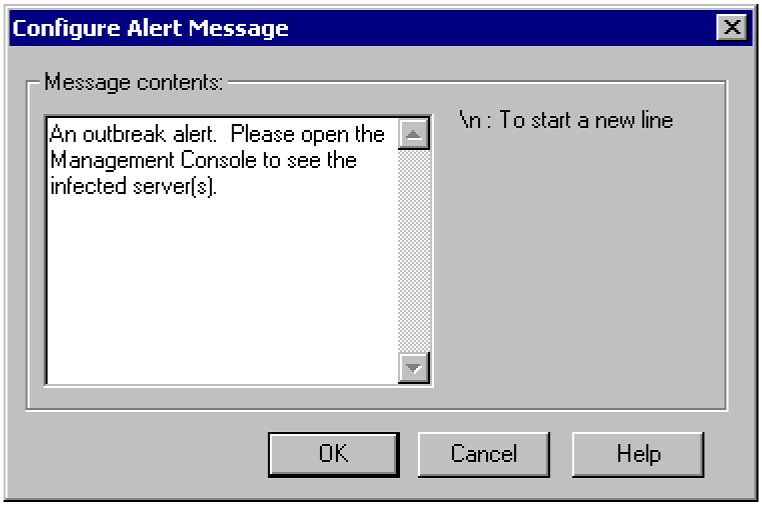
```
Virus pattern on server Tw-sun is out-of-date.
```

Outbreak Alert

A virus outbreak is a large number of virus events that occur over a relatively short period. Outbreak alerts have a high potential for causing damage on a network. If the number of virus events exceeds the threshold that you have defined, an outbreak alert is triggered to notify you.

To generate message text that notifies you of a virus outbreak on your network, you use the following special character to display fields (see Figure 5-8). You then enter your own text to include special information about the outbreak.

- `\n` : start a new line



An outbreak alert. Please open the Management Console to see the infected server(s).

\n : To start a new line

Figure 5-8: Configure Alert Message dialog box

ServerProtect sets the following default characters:

```
An outbreak alert. Please open the Management Console to see the
infected server(s).
```

If you keep the default characters, ServerProtect sends the following message:

```
An outbreak alert. Please open the Management Console to see the
infected server(s).
```

Setting Alert Methods

ServerProtect can notify you about a virus event or an outbreak in several different ways. To ensure that you are notified of virus events or outbreaks, you can configure ServerProtect to use several notification methods at once. You can then take action before a virus causes serious damage to the network.

You can select the following alert methods:

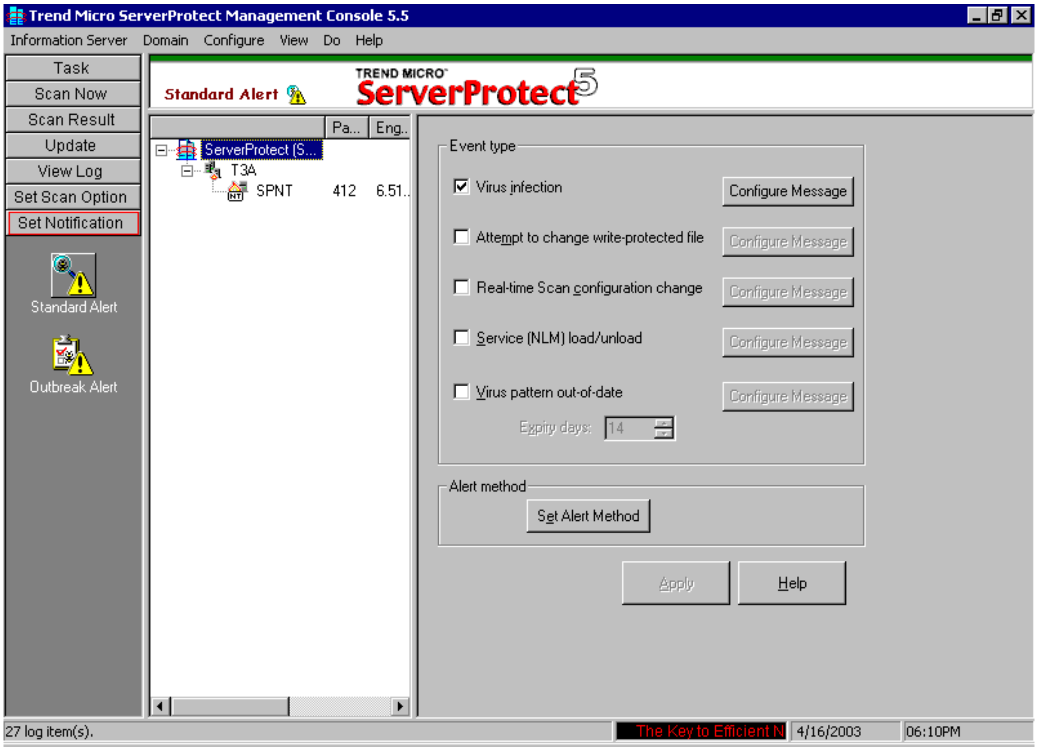
Message-Box Alert A standard Windows pop-up message box is displayed on your screen.

Printer Alert Virus and program alerts can be sent to a network printer to notify people of a potentially serious problem. However, you must first configure ServerProtect to use a particulare printer. You can select only one printer to print the virus alerts.

Pager Alert Virus and program alerts can be sent to any numeric pager. When you are away from your computer, a pager alert is a convenient way to receive alert messages. You can configure two Normal Servers per domain to send out notifications.

Internet Mail (Email) Alert	Virus and program alerts can be sent by Internet email.
SNMP Trap Alert	Simple Network Management Protocol (SNMP) traps are a way of sending virus or program event alerts to a management console that supports SNMP traps. For example, management consoles such as Unicenter from Computer Associates, Hewlett-Packard OpenView, and some products from IBM Tivoli systems support SNMP traps.

You configure alert methods for virus events and outbreak events separately. To configure how ServerProtect notifies you of virus events, select **Set Alert Methods** in the *Standard Alert* configuration window. The dialog box shown in Figure 5-9 appears.



Event type

☑ Virus infection

□ Attempt to change write-protected file

□ Real-time Scan configuration change

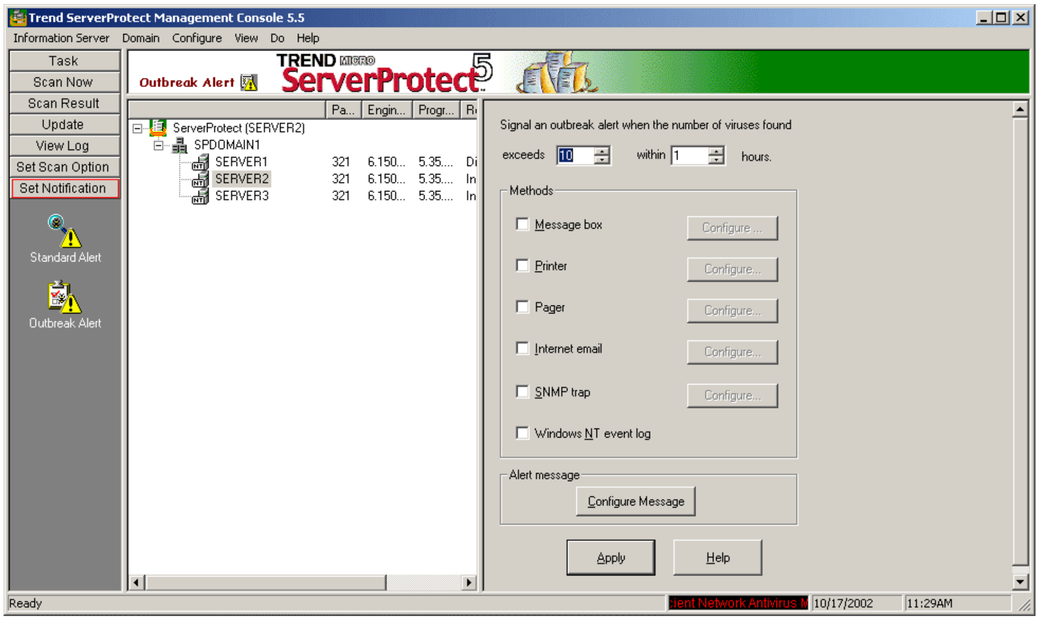
□ Service (NLM) load/unload

□ Virus pattern out-of-date

Expiry days: 14

Figure 5-9: Setting alert methods

To configure how ServerProtect notifies you of an outbreak, select the alert method on the *Outbreak Alert* configuration window.



	Pa...	Engin...	Progr...	R
ServerProtect (SERVER2)				
SPDOMAIN1				
SERVER1	321	6.150...	5.35....	Di
SERVER2	321	6.150...	5.35....	In
SERVER3	321	6.150...	5.35....	In

Signal an outbreak alert when the number of viruses found

exceeds 10 within 1 hours.

Methods

☐ Message box

☐ Printer

☐ Pager

☐ Internet email

☐ SNMP trap

☐ Windows NT event log

Alert message

Figure 5-10: Outbreak Alert Configuration Window

Information for NetWare Users

If the notification printer is installed on a NetWare server, the Information Server that manages the NetWare server must install the same printer as well. Otherwise, the printer alerts cannot be sent properly.

If you want to configure a NetWare server to issue SNMP trap alerts, you need to manually copy ***TMSP.mib*** to the Novell ManageWise directory. (ManageWise is an SNMP management system.) ***TMSP.mib*** is located in the ServerProtect home directory. You must then run the SNMP MIB compiler from ManageWise. After the compilation is completed, you can view SNMP trap alerts from ManageWise.

If Trend Micro Control Manager is installed on your network, turn off its notification functions so that you do not receive duplicate notification messages.

Lab Exercise 3: Configuring Virus Scanning

Chapter 5 Summary and Review Questions

Summary

You configure tasks to use ServerProtect's virus scanning function. When you install a Normal Server, three default tasks are automatically created. You can also use the task wizard to create any task you need. When you configure a scanning task, you specify functions such as the type of scan and the actions that ServerProtect should take against infected files.

Notifications ensure that you are informed immediately if an infected file is detected, if the virus pattern is out-of-date, or if a virus outbreak occurs. You can configure notifications to be sent to a variety of destinations.

Review Questions

1. Which kind of task would you set up if you needed to make sure that all files accessed on a particular server were always scanned?

   a. Scan Now

   b. Deploy

   c. Real-Time Scan

   d. Scheduled Scan

2. Which action should you take against an infected file if you want to prevent the file from being executed or opened?

   a. Bypass

   b. Rename

   c. Move

   d. Clean

3. Which of the following is *not* an event for which you can configure ServerProtect to notify you?

   a. Virus infection

   b. Scan complete

   c. Attempt to modify write-protected file

   d. Virus pattern out-of-date

4. When configuring alert messages, what does the character "\n" mean?

   a. Notification

   b. Name of computer

   c. Name of user

   d. Start a new line