

## Contents



[Introduction](#)



[Scanning for Viruses](#)



[ScanMail Log Files](#)



[Configuring ScanMail](#)



[Updating the Virus Pattern File](#)



[Registering ScanMail](#)



[Technical Support](#)

## Contents



### Introduction

ScanMail for Microsoft Exchange was specifically designed to protect Microsoft Exchange users against all types of computer viruses that can enter their systems via files received as mail attachments.

ScanMail for Microsoft Exchange is installed directly on the Microsoft Exchange server and stops viruses at the server before they have a chance to spread to workstations. ScanMail can check Internet or Intranet e-mail attachments for viruses, depending on how the Microsoft Exchange server is deployed in your corporation. Besides having a real-time scanner which continuously monitors mail attachments for viruses, ScanMail also has a manual scanner and scheduled scans which can scan the whole Exchange server for viruses, including all mail boxes documents and other files shared by Microsoft Exchange users.

### [Features](#)

## ScanMail Features

ScanMail for Microsoft Exchange is designed to detect and clean viruses that are attached to mail messages received through the Microsoft Exchange server. ScanMail continuously monitors incoming Internet and Intranet mail passing through the Microsoft Exchange server, stopping viruses at the server level, before they have a chance to spread.

When ScanMail detects an infected mail attachment, it takes the action configured by the ScanMail administrator.

Main features of ScanMail for Microsoft Exchange include:

- Scans Internet/Intranet traffic - ScanMail scans and cleans viruses attached to Microsoft Exchange mails in real time, as soon as they arrive at the Exchange server.
- Scans all attachments before a user reads or saves them.
- Reduces reinfections - Reinfections by viruses, especially macro viruses, are particularly hard to eradicate because even though you may have stopped the first infection, a copy of the virus could be hidden in an old mail or in a public folder ready to reinfect again. ScanMail for Microsoft Exchange can check old mails, shared documents and public folders on the Exchange server ensuring that there are no hidden viruses ready to reinfect again.
- Detects known AND unknown viruses - ScanMail for Microsoft Exchange makes use of Trends proprietary virus scanning engine, which incorporates both rule-based and pattern recognition technology to provide detection and removal capabilities for more than 8,000 known computer viruses. ScanMail also incorporates MacroTrap, Trends patent-pending generic macro virus trap, which detects and removes known and unknown macro viruses.
- Virtual Virus Hospital - The Virtual Virus Hospital offers personalized diagnosis and cleaning of virus infected files 24 hours a day. Infected files that require extra attention may be e-mailed to Trends Virus Hospital.
- Automatic virus pattern updates - A virus scanner is only as effective as its most recent update, so obtaining frequent virus pattern updates is critical to maintaining a secure computing environment. ScanMail provides convenient automatic pattern updating through the Internet on a daily, weekly, or monthly basis.
- Immediate notifications - Whenever a virus is detected, ScanMail immediately notifies the sender and recipient of the infected file as well as the administrator.
- Fast Performance - The ScanMail program and scanner is multi-threaded, resulting in fast performance yet with minimal system overhead.
- Detects viruses in compressed files - ScanMail can detect viruses hiding in compressed files including files compressed in PKZIP, PKLITE, ARJ, LZH, LHA and Microsoft Compress formats. ScanMail also finds viruses encoded in UUEncoded and MIME format files.
- Easy installation and configuration.
- Can be configured to perform the following tasks:  
Automatically clean infected files, delete them, or quarantine them. Issue notifications to the administrator, recipients, and senders when an infected file is detected.

## Contents



### Scanning for Viruses

You can use ScanMail for Microsoft Exchange to scan for viruses in one of three ways: by using the real-time scanner, by performing a manual scan, or by performing a scheduled scan.

#### **Real-Time Monitor**

[Using Real-Time Monitor](#)

[Viewing Real-Time Monitor](#)

#### **Manual Scan**

[Performing a Manual Scan](#)

[Viewing Manual Scan Results](#)

#### **Scheduled Scan**

The scheduled scan provides you with automatic regulated scanning of your Exchange server. You can set the scheduled scan to scan daily, weekly, or monthly. You can also set multiple scheduled scans.

[Adding a Scheduled Scan](#)

[Modifying Scheduled Scan](#)

[Deleting a Scheduled Scan](#)

## Using the Real Time Monitor

The real-time scanner detects viruses in Microsoft Exchange mail attachments in real time. For the real-time scanner to function it must be enabled. To run and enable the real-time scanner, follow the steps below:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Switch to the Real Time Scan page by clicking on the appropriate tab.
3. To enable the real-time scanner, make sure that the Enable real time scan check box in the top left-hand corner is checked.
4. Configure the options for the real-time scanner by clicking on the Options button. Options include: actions to take on finding a virus, and virus notification messages.

The real-time scanner is now enabled.

## Viewing the Real Time Monitor

The Real Time Scan Monitor shows the current status of the real-time scanner. To view the status of the Real Time Scan Monitor, follow the steps below:

1. Select the item Real Time Scan Monitor located in the ScanMail for Microsoft Exchange program group.

2. The Real Time Scan Monitor shows the following fields:

Real Time Scan Status - Shows information about the real-time scanner, including when it was first started, the configured action taken when viruses are detected, the average processing time, number of messages scanned, the number of infected messages, and the number of viruses found.

Last Virus Found - shows the name of the last virus found.

Messages Scanned - shows a list of the messages that have been scanned by ScanMail. If a virus is detected in a message, ScanMail will show a virus found message in this area.

To clear the messages from the Messages Scanned list, click the Clear Messages button.

## Performing a Manual Scan

The manual scanner can be used to check the Exchange server mail boxes and public folders for any viruses which may be hidden in old mails. It is advised that you run the manual or scheduled scan on a regular basis to ensure that the Exchange server is virus free.

To perform a manual scan, follow these steps:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Select the Manual Scan page by clicking on it.
3. Select the mailboxes you want to scan by placing a check mark next to the item.
4. Select the items in the mail box you wish to scan by filling in the check box next to the appropriate item. Available items include: the Inbox, the Outbox, Sent Items, Deleted Items, and Others (includes all other Folders).
5. Configure the options for the manual scanner by clicking on the Options button. Options include: actions to take on finding a virus, and virus notification messages.
6. Click on the Scan button to begin scanning.
7. This shows the status of the scan. If you wish to cancel the scan, click on the Stop button. Otherwise, no action is required.
8. Once the scan is completed, ScanMail will log the event to the Event Log.

On completion of the scan, if any viruses have been found, ScanMail will automatically switch to the Results page to display detailed information about the detected viruses.

## **Viewing the Manual Scan Results**

If viruses are detected by ScanMail during a manual scan operation, ScanMail will automatically switch to the Results page on completion of the manual scan. The Results page shows detailed information about the scan, including the total number of messages scanned, the number of viruses found, the number of infected messages, and the elapsed scan time. A list box is also shown which contains details of the detected viruses.

To view information about the sender of the infected attachment, select the item and then click on the Sender Info. button.

To view information about the virus, select the virus and then click on the Virus Info. button.



## Adding a Scheduled Scan

To add a scheduled scan, follow the steps below:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Select the Schedule page by clicking on Schedule.
3. To add a scheduled scan, click on the New button.
4. Select the mail boxes you wish to scan by placing a check mark next to the mail box (you can click on the Select All button to select all the mail boxes or click on the Deselect All button to clear all the check boxes).
5. Set the time and date to scan.
6. To configure actions to take on detecting a virus and virus notification messages, click on the Options button
7. Configure the appropriate settings and then click OK to save your changes or Cancel to exit without making any changes.  
You are returned to the Schedule Scan Setting page.
8. Click OK to add the new scheduled scan, or Cancel to quit without adding a new scheduled scan.  
You are returned to the Schedule page.
9. To add additional scheduled scans, repeat Step 3 to Step 8.
10. Make sure that the Enable Scheduled Scan check box in the top left-hand corner is checked.

The scheduled scans are now enabled and will run at the predetermined times.

## Modifying a Scheduled Scan

To modify a scheduled scan, follow the steps below:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Select the Schedule page by clicking on Schedule
3. Select the scheduled scan you wish to modify by clicking on it.
4. Click on the Modify button.
5. Configure the mail boxes you wish to scan by placing a check mark next to the mail box (you can click on the Select All button to select all the mail boxes or click on the Deselect All button to clear all the check boxes).
6. Modify the time and date settings.
7. To configure actions to take on detecting a virus and virus notification messages, click on the Options button.
8. Configure the appropriate settings and then click OK to save your changes or Cancel to exit without making any changes.  
You are returned to the Schedule Scan Setting page.
9. Click OK to save your modifications, or Cancel to quit without modifying the scheduled scan.  
You are returned to the Schedule page.
10. Make sure that the Enable Scheduled Scan check box in the top left-hand corner is checked.

The scheduled scan is modified and will run at the predetermined time.

## **Deleting a Scheduled Scan**

To delete a scheduled scan, follow the steps below:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Select the Schedule page by clicking on Schedule.
3. Select the schedule you wish to delete by clicking on it.
4. Click the Delete button. ScanMail will confirm the deletion.
5. Click Yes to delete the schedule.

The scheduled scan is deleted.

## Contents



### ScanMail Log File

ScanMail creates three types of activity logs that record information about your system including:

**The Event Log** - records the times, dates and events performed by the ScanMail program. This includes all scan events.

**The Virus Log** - contains detailed data on attachments containing virus infected files, including date/time of detection, sender/receiver of the infected attachment and the detection method.

**The Virus Pattern Update Log** - records information about all attempted Virus Pattern File updates.

### Viewing / Deleting the Log Files

[Viewing the Event Log](#)

[Viewing the Virus Log](#)

[Viewing the Virus Pattern Update Log](#)

[Manually Deleting the Log Files](#)

[Automatically Deleting the Log Files](#)

## Viewing the Event Log

To view the Event Log, follow the steps below:

1. Launch the ScanMail main program.
2. Switch to the View Log page by clicking on the appropriate tab.
3. Select the date period that you wish to view by configuring the From and To time fields
4. Select the scan events to show by filling in the Scheduled scan, Manual scan or Real time scan check boxes located below the date field.
5. Click on the Event Log button.
6. The Event Log shows detailed information about all the scan events performed by ScanMail including the date/time of the scan, the type of scan (manual, scheduled), the number of messages scanned, the number of attachments scanned, the number of viruses found, the action taken on infected attachments, and the elapsed scan time.
7. To view details for a particular scan event, select the event and then click on the View Scan Details button
8. A dialog shows the details of the scan:
9. To print the scan details, click on the Print button.
10. To close the scan details dialog, click the Close button.  
You are returned to the Event log dialog.
11. To view a summary of the selected scan event, click the Summary button.
12. Click the Close button to close the dialog.  
You are returned to the Event Log dialog.
13. To print the Event Log, click the Print button.
14. To close the Event Log click the OK button.

## Viewing the Virus Log

To view the Virus Log, follow the steps below:

1. Launch the ScanMail main program.
2. Switch to the View Log page by clicking on the appropriate tab.
3. Select the date period that you wish to view by configuring the From and To time fields.
4. Select the scan events to show by filling in the Scheduled scan, Manual scan or Real time scan check boxes located below the date field.
5. Click on the Virus Log button.
6. The Virus Log shows information about viruses that have been detected by ScanMail, including the date/time, the type of scan that detected the virus (manual or scheduled), the sender of the virus, the recipient of the virus (mail box), the name of the virus, and the action taken on the virus.
7. To view information about the sender, click the Sender button.
8. To view information about the virus, click the Virus Info. button.
9. To print the log, click on the Print button.
10. To close the Virus Log, click the Close button.

## **Viewing the Virus Pattern Update Log**

To view the Virus Pattern Update Log, follow the steps below:

1. Launch the ScanMail main program.
2. Switch to the View Log page by clicking on the appropriate tab.
3. Click on the Update Log button.
4. The Pattern Update log shows information about attempted virus pattern file updates, including the date/time of update, the update method, the version of the pattern file at the source, and the current pattern file version.
5. To print the Pattern Update log, click on the Print button.
6. To close the Pattern Update log, click the Close button.

## Manually Deleting the Log Files

Follow these steps to delete the log files manually:

1. Open the Explorer or File Manager
2. Go to the directory where ScanMail is installed to.
3. There will be a sub-directory called Log. Change to this directory.
4. To delete the Event Log, delete the file:

`scansum.log`

To delete the Virus Log, delete the files starting with the format:

`yearmonthdate.m`, `yearmonthdate.r`, or `yearmonthdate.p`.

e.g `19970115.m`

(m stands for manual scan, r stands for real time scan, and p stands for prescheduled scan).

To delete the Pattern Update Log, delete the file:

`updatptn.log`



## Automatically Deleting the Log Files

Follow these steps to delete the log files automatically:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Switch to the View Log page by clicking on it.
3. Click on the Options button.
4. Select the number of days to keep the records in the log files. The minimum number of days is 1, and the maximum number of days is 90. Old records will automatically be deleted from the log files.  
e.g. If you select to keep the records for 45 days, all records older than 45 days will be deleted from the logs
5. Click the OK button to save your changes.
6. Records will be kept for the selected number of days.

NOTE: Automatic deletion of records in the log files only applies to the Event Log and Virus Log. It does not apply to the Pattern Update Log. To delete information from the Pattern Update Log, please follow the procedure Deleting the Log File Manually on page 5-8.

## Contents



### **Configuring ScanMail**

[Actions on Detecting a Virus](#)

[Notification Messages](#)

[Selecting the ScanMail Profile](#)

## Actions on Detecting a Virus

ScanMail can be configured to deal with viruses automatically. These actions must be pre-configured before the scanning takes place. The actions can be configured in the options setting of the scan program.

The actions that can be set for the manual scan, real-time scan and scheduled scan have identical functions and include:

**Auto Clean** - Automatically attempt to clean the infected attachment file. If the virus is non-cleanable, then either move the infected attachment to the Virus Hospital, to a secure directory, or send it to the ScanMail Administrator for further action.

**Delete** - Automatically delete the virus infected attachment. ScanMail will strip off the attachment containing the virus and delete it.

**Pass** - Perform no action. ScanMail will ignore the virus infected attachment and will only log the results to the Virus Log.

**Move** - Move the virus infected attachment to either the Virus Hospital, a secure directory, or send it off to the ScanMail Administrator.

## Notification Messages

ScanMail can automatically send a virus notification message whenever a virus is detected. Notification messages can be sent to:

- The recipient of the infected attachment.
- The sender of the infected attachment.



The ScanMail Administrator.

The virus notification messages include information such as the name of the detected virus, the subject, the sender/recipient, the date/time, the action taken on the infected attachment (pass, auto-clean, delete or move) and a custom message from the administrator.

The custom message can be configured in the scan options (please refer to Scan Options on page 4-5 for more information).

The default custom messages are:

**To the recipient of a virus infected attachment:**

Warning! A virus has been found in a mail attachment sent to you.

**To the sender of a virus infected attachment:**

Warning! A virus has been found in a mail attachment sent by you.

**To the ScanMail Administrator:**

Warning! A virus has been found.

Trends URL link [www.antivirus.com](http://www.antivirus.com) can also be added to the notification messages allowing users to receive the most up-to-date virus information.

## Selecting the ScanMail Profile

ScanMail requires a Microsoft Exchange profile in order to log on to the server. This profile must have administrator rights to the Microsoft Exchange server. To select a profile for ScanMail, follow these steps:

1. Launch the ScanMail for Microsoft Exchange main program.
2. Switch to the Real Time Scan page by clicking on it.
3. Click on the Profile button.
4. Select an administrator equivalent profile from the drop-down list box.
5. Click OK to save your changes.

ScanMail will use the new profile the next time it is run.

## Contents



### Updating the Virus Pattern File

The Virus Pattern File is used by the virus scanner to detect viruses in files. In order to detect the newest viruses and to keep your virus protection at the highest level possible, it is recommended that you update your Virus Pattern Files frequently.

[Virus Pattern File](#)

[Manually Updating the Virus Pattern File](#)

[Automatically Updating the Virus Pattern File](#)

## **Virus Pattern File**

The ScanMail software contains an extensive virus signature database that is referred to as the Virus Pattern File. ScanMail uses the patterns in this file to detect viruses in mail traffic as well as detecting viruses which may be stored in mail boxes on the Microsoft Exchange server.

Trend Micro Incorporated continuously updates the Virus Pattern File with new signatures, enabling ScanMail to catch the newest viruses. For optimum protection, you should frequently update your Virus Pattern File.

The Virus Pattern File is named LPT\$VPN.xxx where xxx denotes a three digit number (e.g. 203). Higher numbers represent newer releases.

## Manually Updating the Virus Pattern File

To manually update the Virus Pattern File, perform the following steps:

1. Launch the ScanMail main program.
2. Switch to the Update Pattern page by clicking on the appropriate tab.
3. ScanMail gives you three options to update the Virus Pattern File:  
From the Internet - ScanMail automatically downloads the latest Virus Pattern File over the Internet.  
From a Floppy - ScanMail copies the latest Virus Pattern File from the floppy drive.  
From Another Drive - ScanMail copies the Virus Pattern File from the destination specified by the user (this can either be a local path or a network path).
4. Determine the method you want to use to update the Virus Pattern File.
5. To update the pattern through the Internet, click on the Internet button.
6. To update the pattern from the floppy drive or from another path, select the appropriate option from the drop-down list box, then click on the Drives button.
7. ScanMail updates the Virus Pattern File.

You can view the Pattern Update Log for a record of all the pattern updates performed.



## **Automatically Updating the Virus Pattern File**

ScanMail has a Scheduled Pattern Update feature to perform automated periodic Virus Pattern File updates without the need for user intervention. This feature can only update the Virus Pattern File through the Internet or from another Drive. Scheduled pattern update can not be performed from a floppy drive. To automatically update the Virus Pattern File on a periodic basis, perform the following steps:

1. Launch the ScanMail main program.
2. Switch to the Update Pattern page by clicking on the appropriate tab.
3. Enable the scheduled pattern update feature by filling in the Enable Scheduled Update check box.
4. Click on the Options button to configure the frequency and time settings.
5. Select the frequency of the update (weekly or monthly).
6. Configure the time/date/day to perform the update.
7. Click OK to save your changes.

## Contents



### Registering ScanMail

Registered users are entitled to the following benefits:



One year of free updates to the Virus Pattern File.



One year of free technical support.



Free information about future updates and new Trend Micro products.

You can register your ScanMail software by mail, or over the Internet.

[Register by Mail](#)

[Register by the Internet](#)

## **Registering by Mail**

To register by mail, fill out the Registration Card included in the product package and mail it to Trend Micro Incorporated.

## **Registering by the Internet**

To register over the Internet, follow these steps:

1. Launch the ScanMail main program.
2. Switch to the Pattern Update page by clicking on the appropriate tab.
3. Click on the Register button.
4. Fill in all the fields and then click on the Send button to register. Otherwise click the Cancel button to quit.
5. If registration is successful, click on the Finished button.
6. Online registration is now complete

## Contents



### Technical Support

Trend Micro Incorporated provides one year of free technical support for registered users of ScanMail. You can get this support over the telephone, by fax, by e-mail, from the World Wide Web (WWW) page, and by regular mail.

The ScanMail main program provides a list of support numbers and addresses for various locations. To view this list, follow the steps below:

1. Launch the ScanMail main program.
2. Select Technical Support from the Help menu.
3. Select the location nearest you from the Office drop-down list box.
4. The contact information appears in the area below.
5. To print the list, click on the Print button.
6. Click Close to close the dialog box.

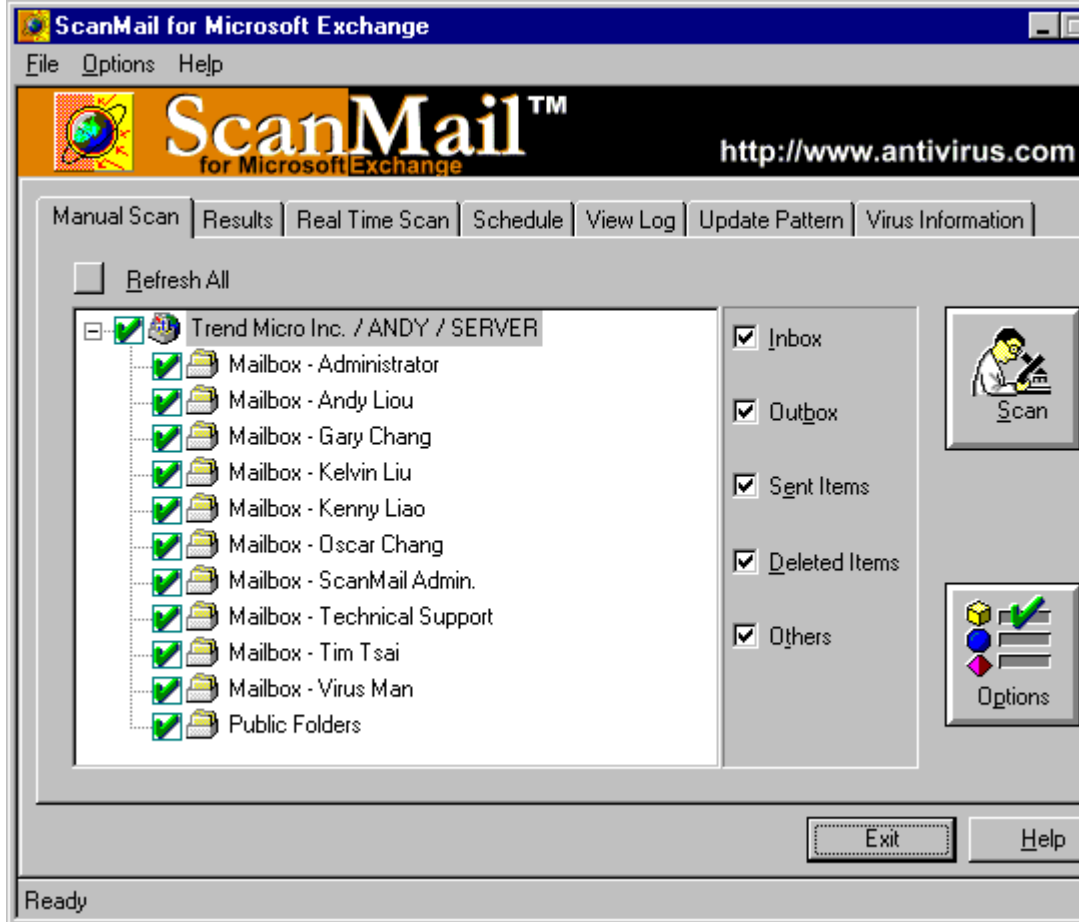
NOTE: If you cannot access the list of support numbers and address from the ScanMail program, please contact:

Trend Micro Inc.,  
20245 Stevens Creek Blvd.  
Cupertino, CA 95014  
U.S.A.  
Tel: (408) 257 1500  
Fax: (408) 257 2003  
Email: [trend@trendmicro.com](mailto:trend@trendmicro.com)

## Scan Page

[Contents](#) [Search](#) [Back](#) [Print](#)

Click on a specific area where you would like more information on.



Click this button to show the latest information about mail boxes on the Microsoft Exchange server. If you cannot see a mail box which you know exists on the Exchange server, clicking the Refresh All button will refresh the screen with the most recent information.

The tree list view shows a hierarchical structure of all mail boxes on the Microsoft Exchange server, including all public and other folders. The tree list view is used to select or deselect mail boxes to scan. To select a Mail box, place a check mark in the box next to the mail box. To deselect a Mail box, remove the check mark.



You can select to scan specific areas of the Mail Box. These include, the Inbox, the Outbox, the Sent Items Folder, the Deleted Items Folder, and Other Folders (including Public Folders).

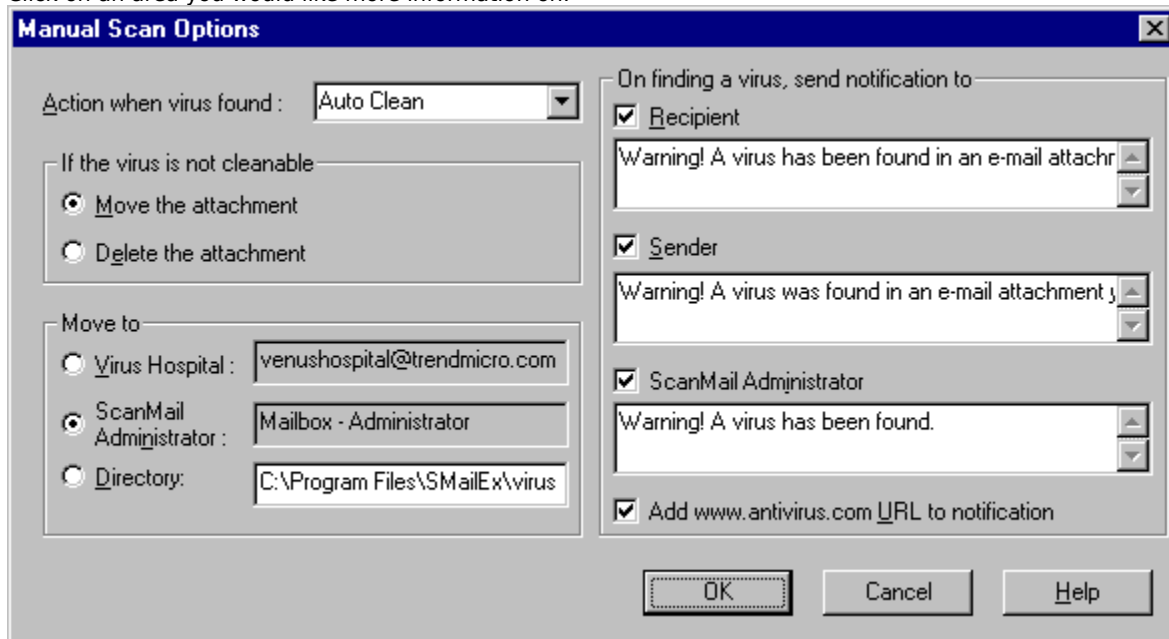
Click this button to begin scanning the selected mailboxes.

Click this button to configure manual scan options

See [Manual Scan Options](#)

## Scan Options

Click on an area you would like more information on.



The image shows a Windows-style dialog box titled "Manual Scan Options". It is divided into several sections for configuring scan actions and notifications.

**Action when virus found:** A dropdown menu is set to "Auto Clean".

**If the virus is not cleanable:** Two radio buttons are present: "Move the attachment" (selected) and "Delete the attachment".

**Move to:** Three radio buttons are present, each with a corresponding text field:

- "Virus Hospital": venushospital@trendmicro.com
- "ScanMail Administrator": Mailbox - Administrator (selected)
- "Directory": C:\Program Files\SMailEx\virus

**On finding a virus, send notification to:** A section with three checked checkboxes and three text fields:

- R**ecipient: Warning! A virus has been found in an e-mail attachr
- S**ender: Warning! A virus was found in an e-mail attachment y
- S**canMail Administrator: Warning! A virus has been found.

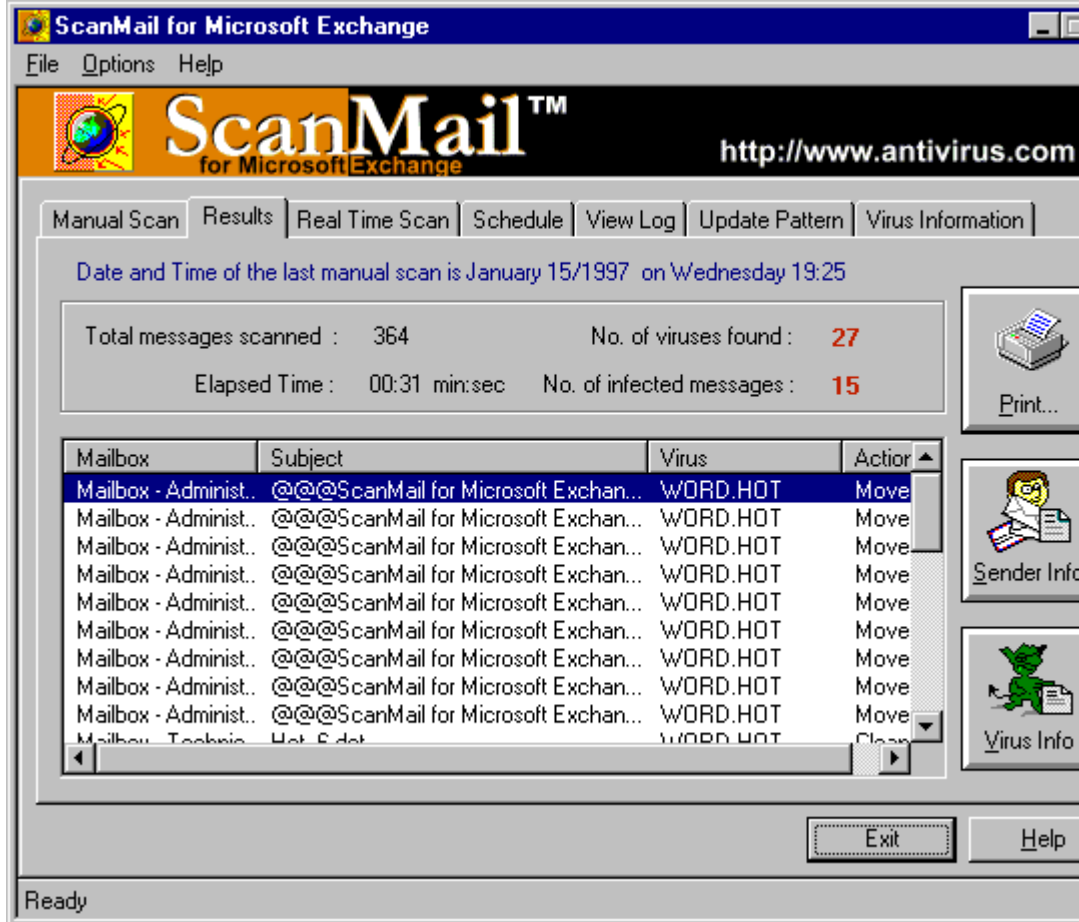
**A**dd [www.antivirus.com](http://www.antivirus.com) **U**RL to notification

At the bottom, there are three buttons: "OK", "Cancel", and "Help".

## Result Page

[Contents](#) [Search](#) [Back](#) [Print](#)

Click on a specific area where you would like more information on.



The screenshot shows the ScanMail for Microsoft Exchange application window. The title bar reads "ScanMail for Microsoft Exchange". The menu bar includes "File", "Options", and "Help". The main interface features a navigation bar with tabs: "Manual Scan", "Results", "Real Time Scan", "Schedule", "View Log", "Update Pattern", and "Virus Information". The "Results" tab is active, displaying the following information:

Date and Time of the last manual scan is January 15/1997 on Wednesday 19:25

Total messages scanned :	364	No. of viruses found :	27
Elapsed Time :	00:31 min:sec	No. of infected messages :	15

On the right side, there are buttons for "Print...", "Sender Info", and "Virus Info". Below the summary is a table listing scan results:

Mailbox	Subject	Virus	Action
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Administr...	@@@ScanMail for Microsoft Exchan...	WORD.HOT	Move
Mailbox - Technic...	Hot E.dat	WORD.HOT	Clean

At the bottom of the window, there are "Exit" and "Help" buttons. The status bar at the very bottom shows "Ready".

This area shows information regarding the last manual scan performed.

This area shows information about all viruses detected by the last manual scan including what actions were taken on the virus. To view sender details or virus details, select the appropriate message and then click on either the Sender Info button or the Virus Info button.

Click this button to print the results of the last manual scan.



Click this button to view information regarding the sender of the selected virus.

Click this button to view more detailed information regarding the selected virus.

## **View Result Log**

The Result Log shows information regarding the selected scan event.

To view information about the sender of a particular virus, select the appropriate virus and then click on the Sender Info button.

To view information about a particular virus, select the appropriate virus and then click on the Virus Info button.

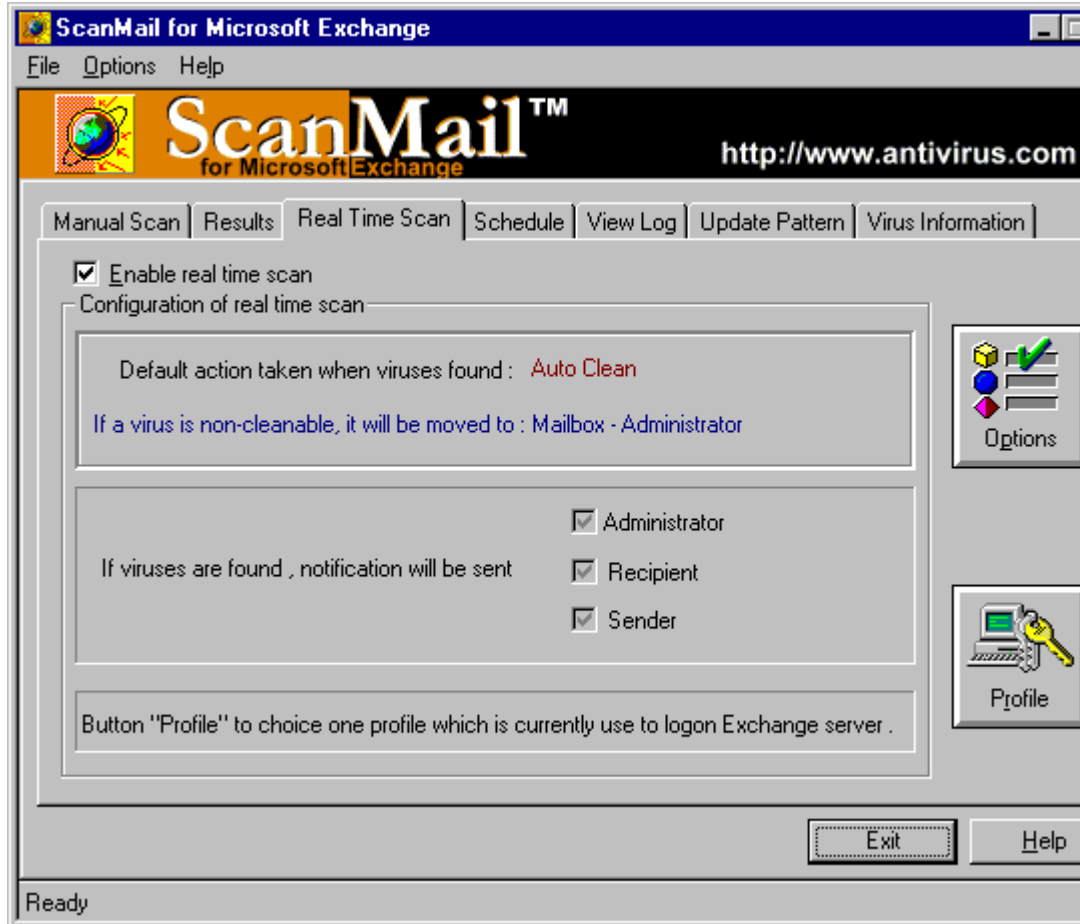
Click on the Print button to print out the virus log.

Click on the Close button to close this dialog.

## Real Time Page

[Contents](#) [Search](#) [Back](#) [Print](#)

Click on a specific area where you would like more information on.



The real time scanner continuously checks all messages for viruses. To enable the real time scanner, fill in the check box. To disable the real time scanner, clear the check box.

This area shows the pre-configured action to take when a virus is found. To configure the action, click on the Options button located on the right hand side of the page.

This area shows details on who will receive notification messages when a virus is detected. You can configure the virus notifications from the Options page.

Click on the button to access the Real Time Options page. Configurable options include actions to take on detecting a virus, and notification messages.



Click on the button to configure which profile is used by ScanMail to log on to the Microsoft Exchange server. The selected profile should have administrator rights to the Microsoft Exchange server.

## Real Time Options

Click on an area you would like more information on.

**Real Time Scan Options**

Action when virus found:

If the virus is not cleanable

Move the attachment

Delete the attachment

Move to

Virus Hospital:

ScanMail Administrator:

Directory:

On finding a virus, send notification to

Recipient

Sender

ScanMail Administrator

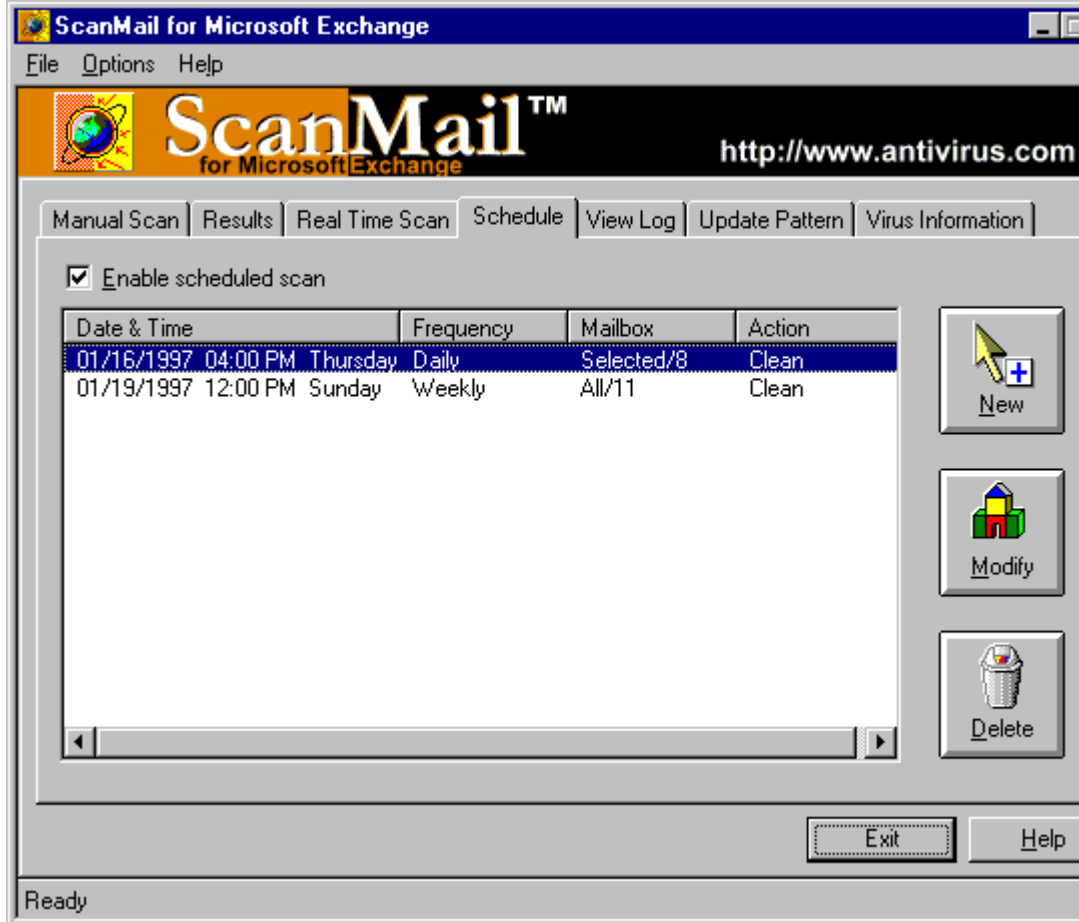
Add www.antivirus.com URL to notification

OK Cancel Help

## Schedule Page

[Contents](#) [Search](#) [Back](#) [Print](#)

Click on a specific area where you would like more information on.



To enable scheduled scanning fill in the check box. To disable all scheduled scans, clear the check box.

This area shows a detailed list of all scheduled scans. To create a new schedule, click on the New button. To modify an existing schedule, select the schedule by clicking on it and then click on the Modify button. To delete a schedule from the list, select the schedule by clicking on it and then click on the Delete button.

Click this button to create a new scheduled scan.

Click this button to modify the selected scheduled scan.

Click this button to delete the selected scheduled scan.



## Add Schedule

Click on an area you would like more information on.

**Schedule Scan Setting** [X]

Select All     Deselect All


- Mailbox - Administrator
- Mailbox - Andy Liou
- Mailbox - Gary Chang
- Mailbox - Kelvin Liu
- Mailbox - Kenny Liao
- Mailbox - Oscar Chang
- Mailbox - ScanMail Admin.
- Mailbox - Technical Support
- Mailbox - Tim Tsai
- Mailbox - Virus Man
- Public Folders

Frequency : Weekly

Time : 12 : 00     AM     PM  
hour    min

Day of Week : Sunday

Day of Month : 1

 Options

OK

Cancel

Help

Click this button to select to scan all the Mail boxes.

Click this button to deselect all the Mail boxes.

This is a list of all available Mail boxes. Mail boxes with a check mark next to them will be scanned for viruses.

Configure the Time and Date settings for the scheduled scan.

Click this button to configure the actions to take when a virus is detected and to configure notification messages.



## Schedule Options

Click on an area you would like more information on.

**Preschedule Scan Options**

Action when virus found :

If the virus is not cleanable

- Move the attachment
- Delete the attachment

Move to

- Virus Hospital :
- ScanMail Administrator :
- Directory:

On finding a virus, send notification to

- Recipient
- Sender
- ScanMail Administrator
- Add www.antivirus.com URL to notification

OK Cancel Help



Select an action to take on detected viruses from the drop-down list box.  
Available actions include Pass (do nothing), Clean, Move or Delete.

If the virus is not successfully cleaned, you can either delete the virus or move the virus to a safe location for further processing.

There are three locations to move viruses to:

**Virus Hospital** - Trends Virus Hospital will analyse the virus and a solution will be emailed back to you. This option is only available to registered users.

**ScanMail Administrator** - The virus will be moved to the ScanMail Administrators Mail box.

**Directory** - The virus will be moved to the specified directory.

On finding a virus, notification messages can be sent to the receiver of the virus, the sender of the virus and to the ScanMail Administrator. To send virus notification messages, fill in the appropriate check box.

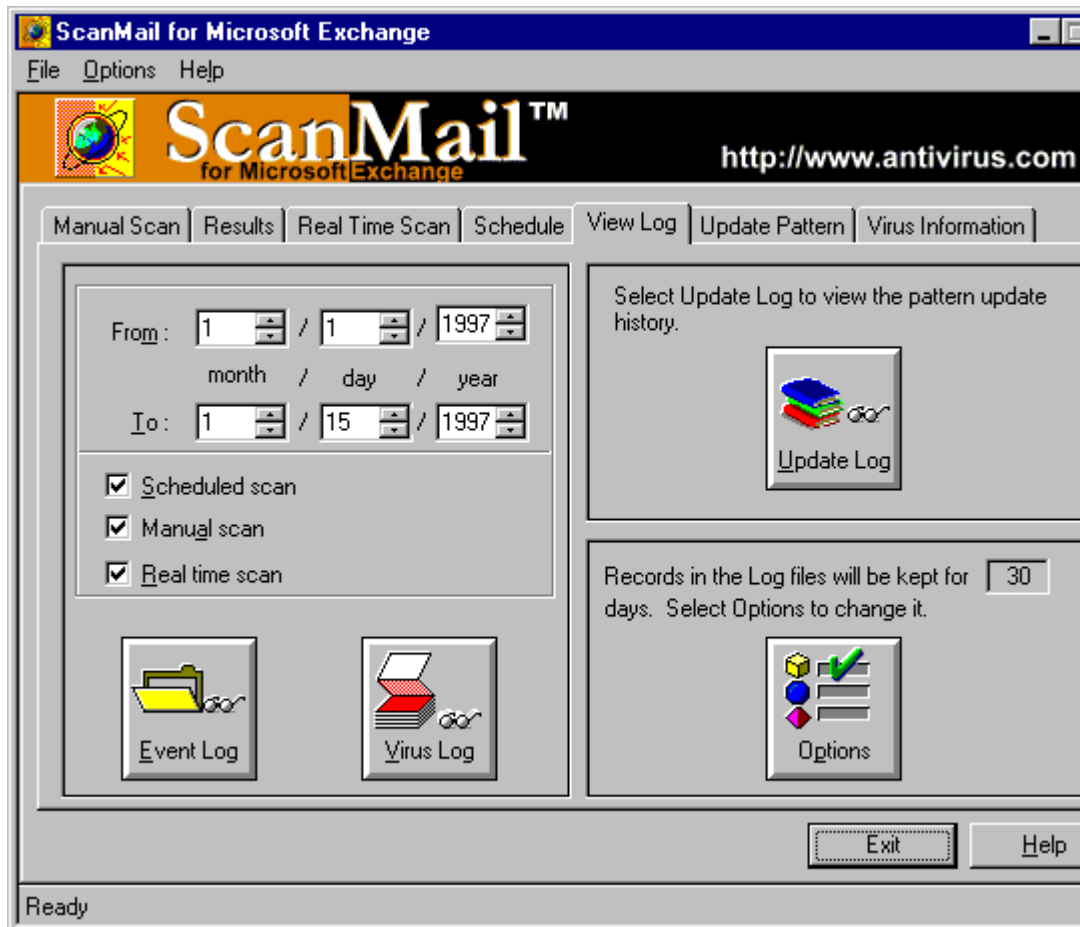
A default warning message is provided which can be customized.

The [www.antivirus.com](http://www.antivirus.com) URL can be added to all virus notification messages. To enable this feature, fill in the check box. To disable this feature, clear this check box.

## View Log Page

• • • •

Click on a specific area where you would like more information on.



Select the starting date you wish to view from.

Select the ending date you wish to view to.



Select which type of scan details you wish to view by filling in the appropriate check box. Available items include: information about schedule scans, information about manual scans, and information about real-time scans or any combination of these three.

Click this button to view the Event Log. The Event Log shows details of all ScanMail scanning events.

Click this button to view the Virus Log. The Virus Log shows details about all the viruses that have been detected.

Click the button to view the Virus Pattern Update Log. The Virus Pattern Update Log shows information about all virus pattern updates.

Click the button to configure how many days to keep information in the log files for. The maximum number of days is 90 days.

## **Event Log**

The Event Log shows information regarding all the scanning events performed by ScanMail.

To view information about a particular scanning event, select the appropriate event and then click on the View Scan Details button.

To view summary information about the Event Log, click on the Summary button.

Click on the Print button to print out the virus log.

Click on the Close button to close this dialog.

## **Virus Log**

The Virus Log shows information regarding all the viruses that have been detected by ScanMail.

To view information about the sender of a particular virus, select the appropriate virus and then click on the Sender Info button.

To view information about a particular virus, select the appropriate virus and then click on the Virus Info button.

Click on the Print button to print out the virus log.

Click on the Close button to close this dialog.

## **View Log Options**

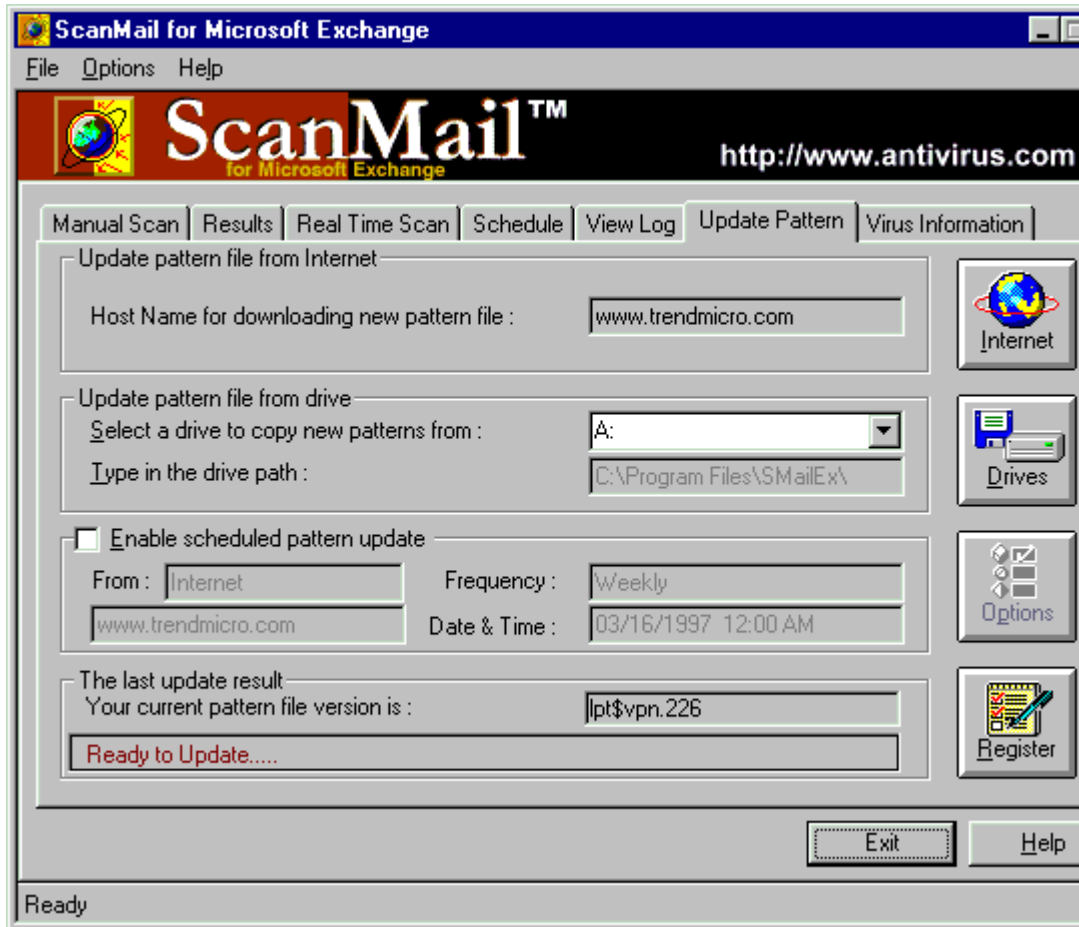
Select the number of days to keep records in the log files for. The maximum number of days that records can be kept for is 90 days.



## Update Pattern Page

• • • •

Click on a specific area where you would like more information on.



This area shows the site where Internet pattern updates are made from. The details shown are for reference only and are not configurable.

This area shows information regarding updating the virus pattern file from a local drive or network drive. Downloads can be performed from the A drive the B drive or from another driver. If you specified another drive, you must type in the drive details in the drive path input box. Other drives can include hard drives or network drives and UNC paths are acceptable.

To enable the schedule pattern update, fill in this check box. To disable scheduled pattern updates, clear this check box.

This area shows information about the schedule pattern update.

This shows the version number of your current virus pattern file. The higher the number, the newer the pattern file.

This area shows the current status of virus pattern updates.

Click this button to download the latest virus pattern file from the Internet.

Click this button to download the latest virus pattern file from the specified drive.

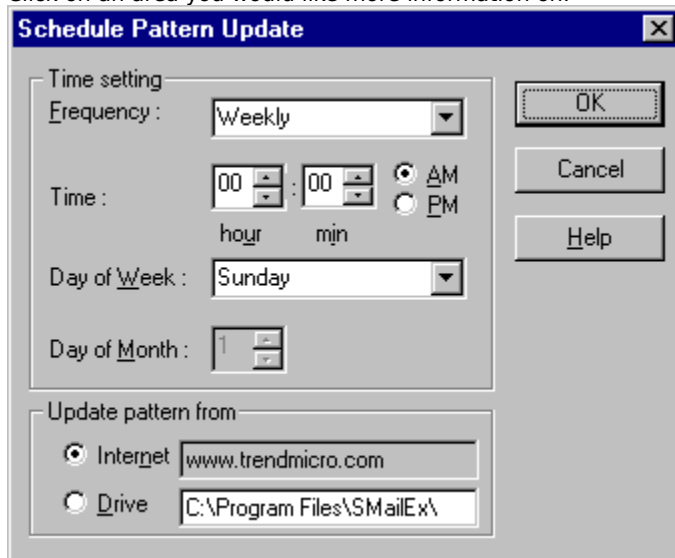


Click this button to configure the schedule pattern update options.

Click this button to perform online registration of ScanMail for Microsoft Exchange.

## Update Pattern Options

Click on an area you would like more information on.



The image shows a Windows-style dialog box titled "Schedule Pattern Update". The dialog is divided into two main sections. The top section, "Time setting", contains a "Frequency" dropdown menu set to "Weekly", a "Time" field with two spinners for hours and minutes (both set to "00"), and radio buttons for "AM" and "PM". Below this is a "Day of Week" dropdown menu set to "Sunday" and a "Day of Month" spinner set to "1". The bottom section, "Update pattern from", has two radio buttons: "Internet" (selected) with a text box containing "www.trendmicro.com", and "Drive" with a text box containing "C:\Program Files\SMailEx\". On the right side of the dialog, there are three buttons: "OK", "Cancel", and "Help".

**Schedule Pattern Update**

Time setting

Frequency : Weekly

Time : 00 : 00 AM

Day of Week : Sunday

Day of Month : 1

Update pattern from

Internet www.trendmicro.com

Drive C:\Program Files\SMailEx\

OK

Cancel

Help

Configure the Time and Date settings for the schedule pattern update.

Configure the pattern update source location. Updates can be made from either the Internet or from a drive (either local or network).

Click this button to close this dialog and save any changes that have been made.

Click this button to close this dialog without saving any changes that have been made.

## **Update Pattern Log**

The Update Pattern Log shows information regarding all virus pattern updates including the date/time of update, the method of update, the version of the virus pattern file at the source, the current virus pattern version and the result of the update (shown in the Updated Result field).

Click the Print button to print out this information.

Click the Close button to close this dialog.



## Virus Information Page

• • • •

Click on a specific area where you would like more information on.



Select the category of viruses you would like to view. Available categories include Common Viruses, Boot Viruses, File Viruses, Macro Viruses or All Viruses.

This is an alphabetical list of all viruses in the selected category. To view information about a particular virus, click on the virus name.

Click on this button to print out information about the selected virus.

Shows information regarding the type of file virus.

Show information regarding the type of memory the virus uses.

Shows a detailed description of the selected virus. To print out this description, click on the Print button.

## **Detectable List**

This is a list of all viruses detectable using the current virus pattern file. There are four categories of viruses including Boot Viruses, File Viruses, Macro Viruses and All Viruses.

You can configure the number of columns of information to show using the slider control located on the top right hand of the dialog.

Click the Save As button to save this information to a text file.

Click the Print button to print out this list of detectable viruses.

Click the Close button to close the detectable list dialog.

## **Event Log Summary**

The Event Log Summary shows a summary of the scan event information for the selected start and end dates.



## Select Profile

ScanMail requires a profile in order to log on to the Microsoft Exchange server. Select a profile from the drop-down list box. This profile must have administrative rights to the Microsoft Exchange server.

