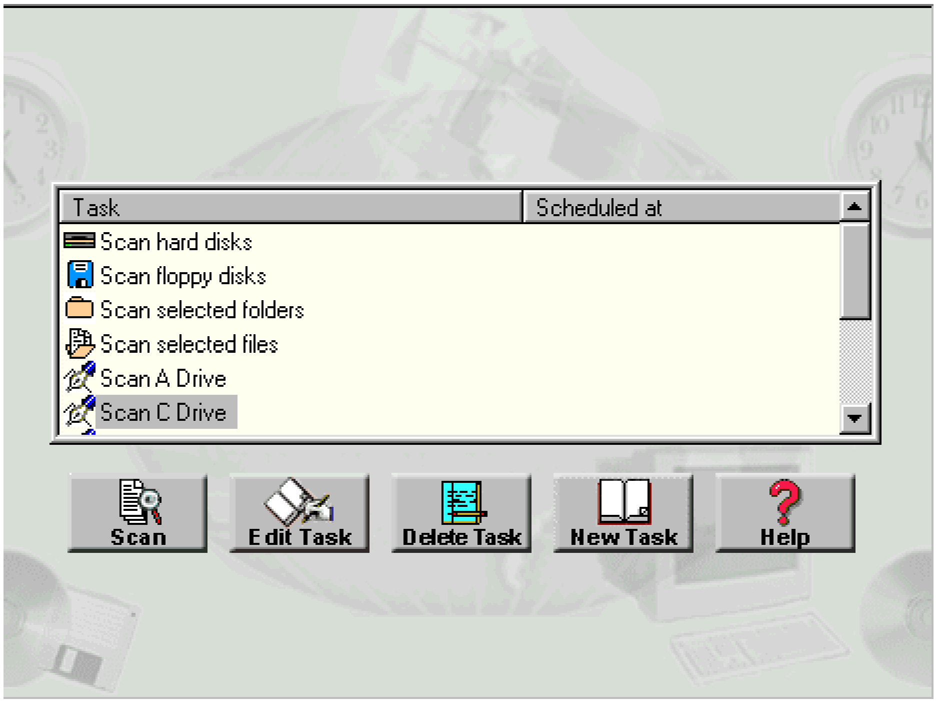
The Manual Scanner

Protector Plus manual scanner can check the computer for viruses, trojans and worms of all kinds. The manual scanner can check entire drives, or a select group of files or folders, whenever required.

A group of files or folders can be grouped under a single scan task and given a name. These user defined scan tasks are displayed in the scan window, below the default scan task list.

All scan tasks can be performed at will or scheduled to run at pre-set intervals.

For context sensitive help, please click on specific items of interest in the image below:



Task	Scheduled at
Scan hard disks	
Scan floppy disks	
Scan selected folders	
Scan selected files	
Scan A Drive	
Scan C Drive	

Manual Scan

A virus has been found during the scan. You can tell the scanner to take any of the actions that are possible. The options are

Disinfect

The scanner will remove the virus code from the infected file, leaving a clean and working file.

Delete

The scanner will delete the infected file from the hard drive.

Rename

The file is renamed and saved in the same folder. (eg. *.EXE is renamed to *.VXE)

Quarantine

The infected file is moved to the Quarantine folder, created under the Protector Plus folder as QUARANTN. More information on the Quarantine process can be viewed here.

Ignore

The scanner will not take any action on the infected file

Apply the selection made in this window to the entire scan

Enabling the check box provided against this option will enforce the selection you are making now, as the default course of action the scanner will take if more viruses are found in this session. The scanner will not pop up the prompt window anymore in this session.

Manual Scan

The Manual Scanner is checking for virus in the folders that are being scanned. The Scanning Statistics window gives information on the total number of files that have been checked at any point, the number of viruses found till then, and the corrective action taken by the scanner.

Also displayed is the name of the folder or file that is currently being checked. The entire path where the folder or file is located is displayed.

Manual Scan

The Manual Scanner has completed checking the computer for virus as per the Scan task selection. The scan statistics for this session of the manual scan are displayed.

A Scan Report is generated for the current session of the scan. This report can be viewed immediately by clicking on the Scan Report button. The entire Scan History can be viewed by clicking on the Scan History button.

Please note that the scan report is generated and a history is maintained only if it is set up in the Manual Scan options

Highlight the Scan task to be performed and then click on this button to initiate the Manual Scan process.

Click on this button to delete the selected Manual Scan task.

Scan Hard Drive

Checks the entire hard drive for viruses.

1. Select the Scan Hard Drive option.
2. Double click on the Scan Hard Drives option or click on the Start Scan button.

Scan a Floppy

Checks a floppy disk for viruses

1. Insert the floppy you want checked for virus into the drive.
2. Select the Scan a Floppy option.
3. Double click on the Scan a Floppy option or click on the Start Scan button.

Adding a user defined task

Defining a Specific Scan Task

Manual Scan tasks can be user defined. A set of folders or files can be grouped under a scan task and given a name. For example, all download directories can be grouped under a single task and given a name. Manual Scans to check such user defined groups for viruses can be initiated at any time, and also scheduled to run at pre-set intervals.

To define a task,

1. Click on the New Task button in the main Scan window.
2. In the Task Configuration window displayed, enter a name for the new task in the Name slot. (eg., Scan Email Directories).
3. Click on the Add Folder or Add Files icon.
4. From the browser window displayed, select the folder or files that you want to add to the Folders/Files to be scanned list. Multiple folders and files can be grouped under one task.

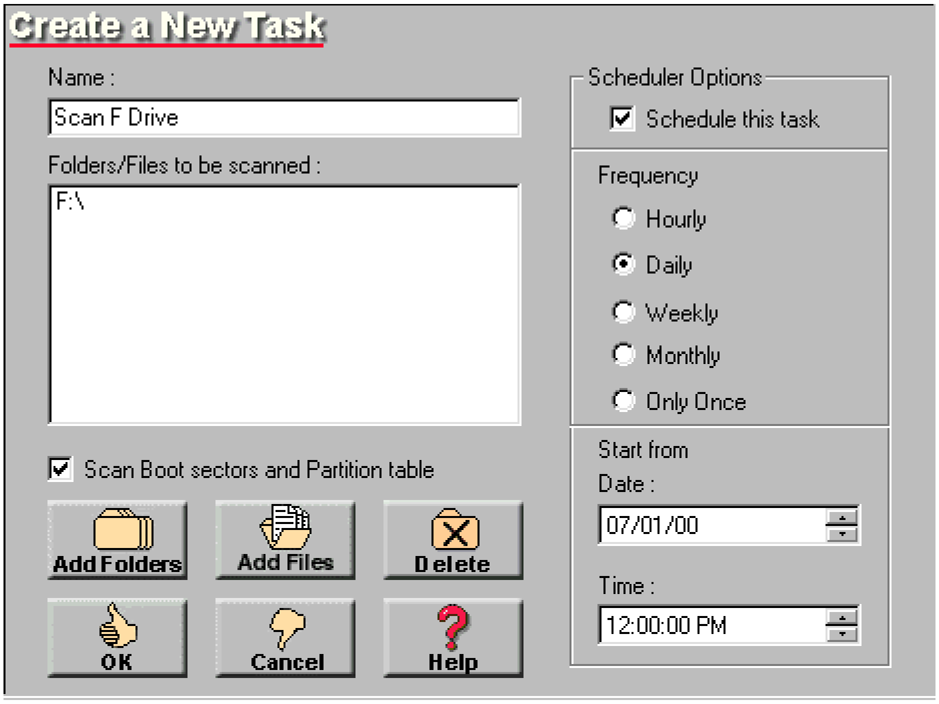
Scheduling a Scan Task

The Manual Scan can be run at pre-set intervals to check for viruses for user defined Scan Tasks. The scan can be scheduled to check the folders/files in that task, hourly, daily, weekly or monthly. Different user defined tasks can be run at different schedules.

To schedule a Scan Task

1. Once you have finished defining a scan task, click on the Protector Plus virus scanning scheduler.
2. In the screen displayed, select the frequency with which you want the scan task performed. Scans can be performed hourly, daily, weekly, monthly, once only at a particular time and date, or none at all.
3. Enter the time at which the Scan Task should be initiated.
4. In the date field, enter the date on which the Scan Task should be initated.

The time and date entered become the reference for the Scheduler to perform the Scan Task. For example, if a Scan Task , ' Scan Email Attachments', is scheduled to run once in a day, at 10.30 in the morning starting on 2/28/2000, the Manual Scan will perform that task every day at 10.30 in the morning, starting from the 28th of February 2000.



Create a New Task

Name : Scan F Drive

Folders/Files to be scanned : F:\

☑ Scan Boot sectors and Partition table

Scheduler Options

☑ Schedule this task

Frequency

○ Hourly
● Daily
○ Weekly
○ Monthly
○ Only Once

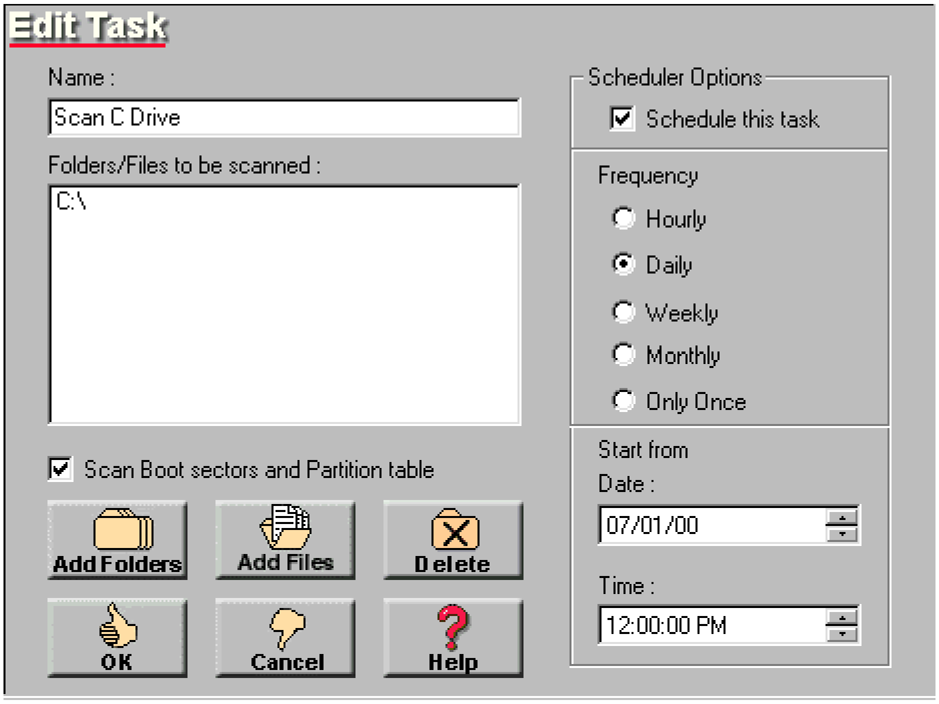
Start from

Date : 07/01/00

Time : 12:00:00 PM

Editing an user defined task

Through the Edit Task module, an existing user defined Manual Scan task can be altered. The name of the task, the folders or files that are to be scanned and the pre-set scan schedules, all can be changed.



Edit Task

Name : Scan C Drive

Folders/Files to be scanned : C:\

☑ Scan Boot sectors and Partition table

Scheduler Options

☑ Schedule this task

Frequency

○ Hourly
● Daily
○ Weekly
○ Monthly
○ Only Once

Start from

Date : 07/01/00

Time : 12:00:00 PM

Enter the name you wish to call the new Manual Scan task.

Edit the name you wish to call the existing Manual Scan task.

Lists all the folders and files that are grouped under the Manual Scan task that is currently selected.

Scanner checks for Boot Sectors and Partition table when this option is enabled.

You can add desired folders to be scanned from the scanner.

You can add desired files to be scanned from the scanner.

Deletes the selected folder(s) or file(s) from the Manual Scan task.

Click on the OK button to save the current settings

Click on the Cancel button to discard changes made in the current session and return the settings to previous state.

Click this button to see help for this topic.

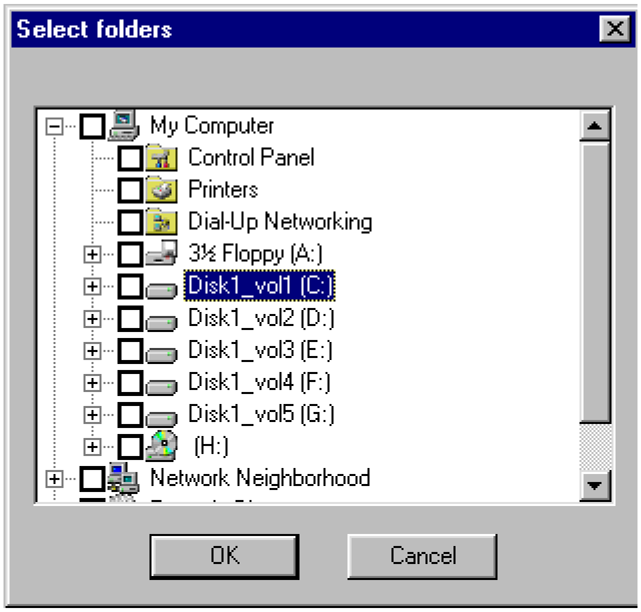
Click on the Check box to enable/disable the Manual Scan task to run at pre-set intervals.

The frequency with which the Manual Scan checks the selected task for virus can be once in an hour, a day, a week or a month. The scheduled task can also be configured to run only once, at the time of entered in the, 'Start from' window. This frequency is selected by clicking on the radio buttons displayed in the menu. The radio buttons are selectable only if the, 'Schedule this task', option is enabled.

Enter the date and time from which the Manual Scan should be initiated for the selected task.

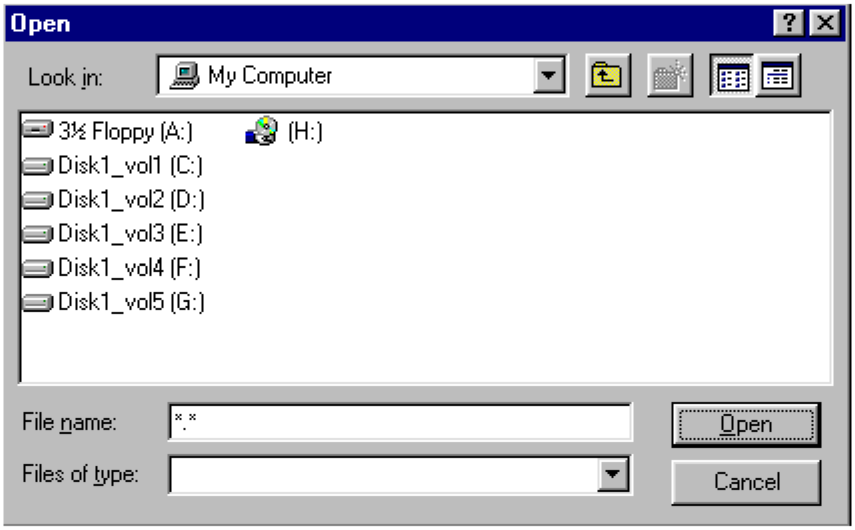
Select Folders

Click on the check boxes to group the folder under the specific Manual Scan task. Directory trees can be expanded by clicking on the + sign displayed against the directory name. The selected folder(s) is (are) displayed in the, 'Folders/files to be scanned', window once the 'OK' button is clicked in the Select folders window.



Select Files

Click on the folder icons to display files in that folder. Select the file to be added to the Manual Scan task by clicking on the file and then clicking on the 'Open' button at the bottom of the window. Multiple files can be added by depressing the Control key while making the selections.



Look in: My Computer

File name: *.*

Files of type:

To define a task, Click on the New Task button in the main Scan window. In the Task Configuration window displayed, enter a name for the new task in the Name slot.

Click on the Add Folder or Add Files icon. From the browser window displayed, select the folder or files that you want to add to the Folders/Files to be scanned list. Multiple folders and files can be grouped under one task.

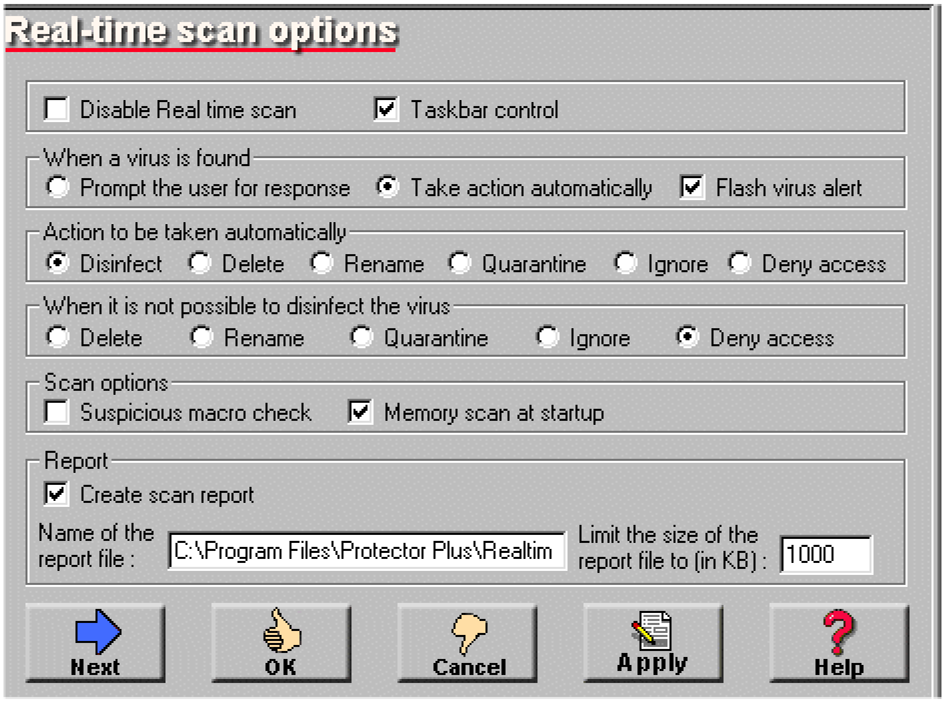
Options

The scanning programs, the Real Time Scanner , Manual Scanner   and the Email Scanner detect viruses. Both these scanners are configurable and are highly flexible. The configuration procedure and the terminology used in the process are simple and easy to understand.   Protector Plus can take user specified action whenever these scanners detect a virus.

Real Time Scan

Whenever a file is accessed, downloaded, copied or created newly, the Real-time Scanner checks that file for virus. The Real-time Scanner is highly flexible and can be customized to suit individual environments.

Configuring Real Time Scan



Real-time scan options

□ Disable Real time scan ☑ Taskbar control

When a virus is found

○ Prompt the user for response ● Take action automatically ☑ Flash virus alert

Action to be taken automatically

● Disinfect ○ Delete ○ Rename ○ Quarantine ○ Ignore ○ Deny access

When it is not possible to disinfect the virus

○ Delete ○ Rename ○ Quarantine ○ Ignore ● Deny access

Scan options

□ Suspicious macro check ☑ Memory scan at startup

Report

☑ Create scan report

Name of the report file : C:\Program Files\Protector Plus\Realtim

Limit the size of the report file to (in KB) : 1000

Click on the radio button, for the Real-time or Email scanner to ask the user for a response when a virus is found. The choices to be displayed can be selected by clicking on the check boxes against them. Please note that these check boxes are displayed only when the real-time scanner has to be prompted by the user to take action, on finding a virus.

Click on the radio button for the Real-time or Email Scanner to take action automatically when it finds a virus. The Protector Plus Scanner can automatically disinfect, delete, rename, quarantine, ignore or deny access to the file. Only one course of action can be selected, by clicking on the appropriate radio.

If the scanner has been set to automatically disinfect viruses detected by it, and due to some reason it is unable to do so, then it can be further automated to take the following course of action. It can automatically delete, rename, quarantine, ignore or deny access to the file. Only one course of action can be selected.

When the check box is enabled, the Scan will flash a virus alert to the user whenever a virus is detected.

Use this checkbox to disable the Real Time scan. When the Real Time Scan is disabled, Protector Plus will not be monitoring the computer in an on-access mode.

When the Task Bar Control is enabled by clicking on the check box, Protector Plus can be loaded into the Task Bar. All functions of the program can be controlled from the Task Bar Control.

Whenever a virus is found in real time, Protector Plus can be configured to prompt the user with alternative courses of action . Only those prompts that are selected will be displayed when a virus is found. The courses of action are Disinfect, Delete, Rename, Quarantine, Ignore or Deny Access to the File.

The Real Time Scan can be automated to take a certain course of action when a virus is detected. On detecting a virus, it can automatically, Disinfect, Delete, Rename, Quarantine, Ignore or Deny Access to, the infected File.   In case it is configured to automatically disinfect an infected file and it is unable to do so, subsequent action can be automated as well. Files that cannot be disinfected can be Deleted, Renamed, Quarantined, Ignored, or locked (denied access to).

When this option is enabled, the scanner will check all documents, XLS and PPT files for the presence of suspicious macros.

When this option is enabled, the Real-Time Scanner checks memory for Viruses, Trojans and Worms, during startup.

Each time the Real Time Scanner detects a virus, a report is generated. This report contains the following information; name of the infected file, name of the virus found, time the infection was detected and the action taken by the Real Time Scanner.

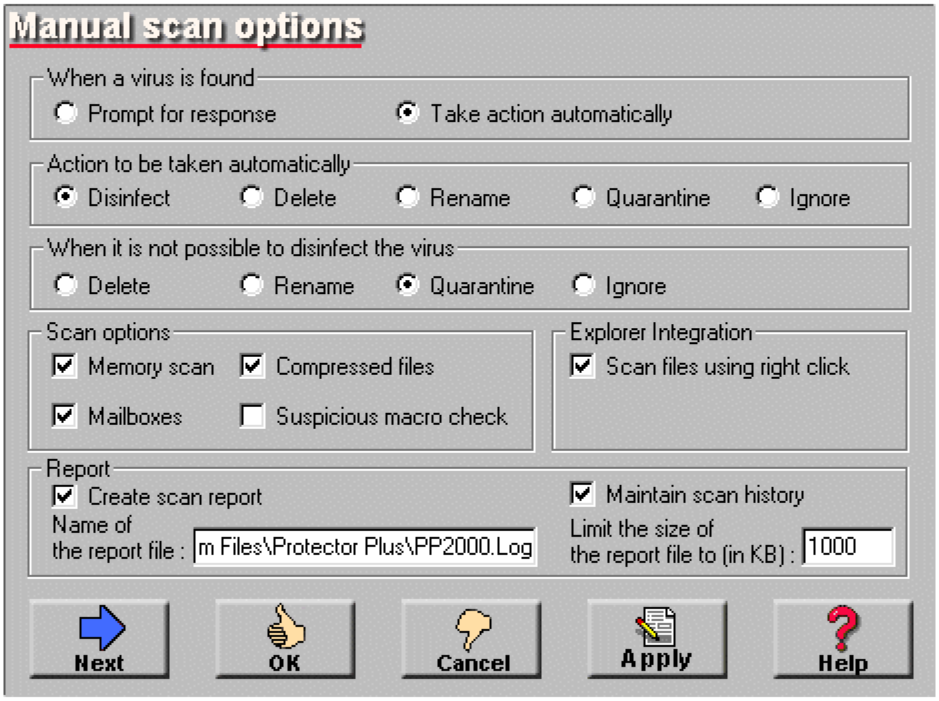
By default, the file is stored under Protector Plus installed directory and is called Realtime.Log. The default size limit is 1000k. The name of the report file and it's size can both be altered.

Saves the changes made and applies them only to the current session. The settings will revert to the previous state in the next session.

Manual Scan

A scan can be initiated at any point. Such user initiated scans are called Manual Scans.

Configuring Manual Scan



Manual scan options

When a virus is found

○ Prompt for response ● Take action automatically

Action to be taken automatically

● Disinfect ○ Delete ○ Rename ○ Quarantine ○ Ignore

When it is not possible to disinfect the virus

○ Delete ○ Rename ● Quarantine ○ Ignore

Scan options

☑ Memory scan ☑ Compressed files

☑ Mailboxes □ Suspicious macro check

Explorer Integration

☑ Scan files using right click

Report

☑ Create scan report

Name of the report file : m Files\Protector Plus\PP2000.Log

☑ Maintain scan history

Limit the size of the report file to (in KB) : 1000

When a virus is detected by the Manual Scan, Protector Plus can be configured to prompt the user with alternative courses of action . Only those prompts that are selected will be displayed when a virus is found. The courses of action are Disinfect, Delete, Rename, Quarantine or Ignore, the File.

The Manual Scan can be automated into taking a certain course of action when a virus is encountered. On encountering a virus, it can automatically, Disinfect, Delete, Rename, Quarantine or Ignore, the infected File.   In case it is configured to automatically disinfect the file and it is unable to do so, subsequent action can be automated as well. Files that cannot be disinfected can be deleted, renamed, quarantined or ignored.

Each time the Manual Scanner detects a virus,   a report is generated. This report contains the following information; name of the infected file, name of the virus found, time the infection was detected and the action taken by the Manual Scanner.

A history of such reports can be maintained. By default, the file is stored under the TEMP directory under WINDOWS and is called Report.doc. The default size limit is 1000k. The name of the report file and it's size can both be altered.

The Manual Scan will check mailboxes and attachments if the Scan Mail Boxes option is enabled.

The Manual Scan will check within compressed files if this option is enabled. It can scan inside *.zip files. Please note that the scanner will only detect viruses in zipped files, but cannot remove them.

When a virus is detected by the Manual Scan, Protector Plus can be configured to prompt the user with alternative courses of action . Only those prompts that are selected will be displayed when a virus is found. The courses of action are Disinfect, Delete, Rename, Quarantine or Ignore, the File.

The Manual Scan can be automated into taking a certain course of action when a virus is encountered. On encountering a virus, it can automatically, Disinfect, Delete, Rename, Quarantine or Ignore, the infected File.   In case it is configured to automatically disinfect the file and it is unable to do so, subsequent action can be automated as well. Files that cannot be disinfected can be deleted, renamed, quarantined or ignored.

When this option is checked, each time the Manual Scanner detects a virus,   a report is generated. This report contains the following information; name of the infected file, name of the virus found, time the infection was detected and the action taken by the Manual Scanner.

A history of scan reports can be maintained. By default, the file is stored under the Protector Plus directory and is called pp2000.log. The default size limit is 1000k. The name of the report file and it's size can both be altered

Manual Scan report file is stored under the Protector Plus directory and is called pp2000.log. The name of the report file and can be altered.

Manual Scan report file is stored under the Protector Plus directory and is called pp2000.log. The default size limit is 1000k. The size of the report file and can be altered.

Files to be Scanned

By default, only those files that are susceptible to virus infection are checked for by the Scanner. All files, irrespective of extension, are checked for virus if the All Files radio button is enabled.

Specific file extensions can be added to the scan list , in addition to the susceptible files that are always checked by   default. Follow these steps to include them in the scan list.

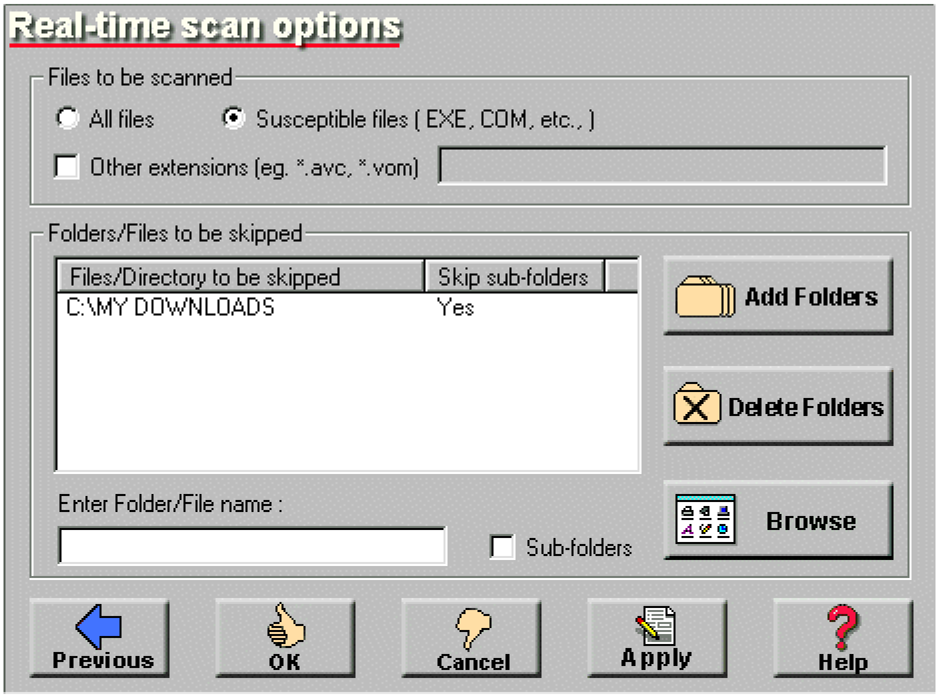
1. Enable the Other Extensions switch, by right clicking the mouse button.   In the box, enter the extension to be scanned. Standard wildcards, like *.VOM, AB*.EXE, etc., are accepted.
2. Once you have completed entering the file extensions you want scanned for virus, click on the OK button to save and exit. Clicking on the Apply button will save the settings only for the current session.

Folders/Files to be skipped

Folders or Files that are added to this list are not checked for viruses by the Scanner. To stop the Scanner from checking a file for virus, follow these steps.

1. Go to Folders/Files to be Skipped. In the field that says Enter Folder/File name, type the name of the file that is not to be checked, along with the path. Click on the Add Folders button. The extension is displayed in the main window. Alternatively, you can also browse and pick up the file you want added by clicking on the Browse button. Standard wildcards, like *.VOM, AB*.EXE, etc., are accepted.
2. If the path terminates in a folder, then the entire folder is not checked for virus.   Under each folder, sub-folders can be checked or skipped by the Scanner depending on whether the Sub-folder option is disabled or enabled. them
3. If the session is done, click on the OK button to save and exit. Clicking on the Apply button will save the settings only for the current session.

It is recommended that this feature be used with extreme caution. Files that are to be skipped will not be scanned for viruses.



Real-time scan options

Files to be scanned

○ All files ● Susceptible files (EXE, COM, etc.,)

□ Other extensions (eg. *.avc, *.vom)

Folders/Files to be skipped

Files/Directory to be skipped	Skip sub-folders
C:\MY DOWNLOADS	Yes

Enter Folder/File name :

□ Sub-folders

Files to be Scanned

By default, only those files that are susceptible to virus infection are checked for by the Scanner. All files, irrespective of extension, are checked for virus if the All Files radio button is enabled.

Specific file extensions can be added to the scan list , in addition to the susceptible files that are always checked by default. Follow these steps to include them in the scan list.

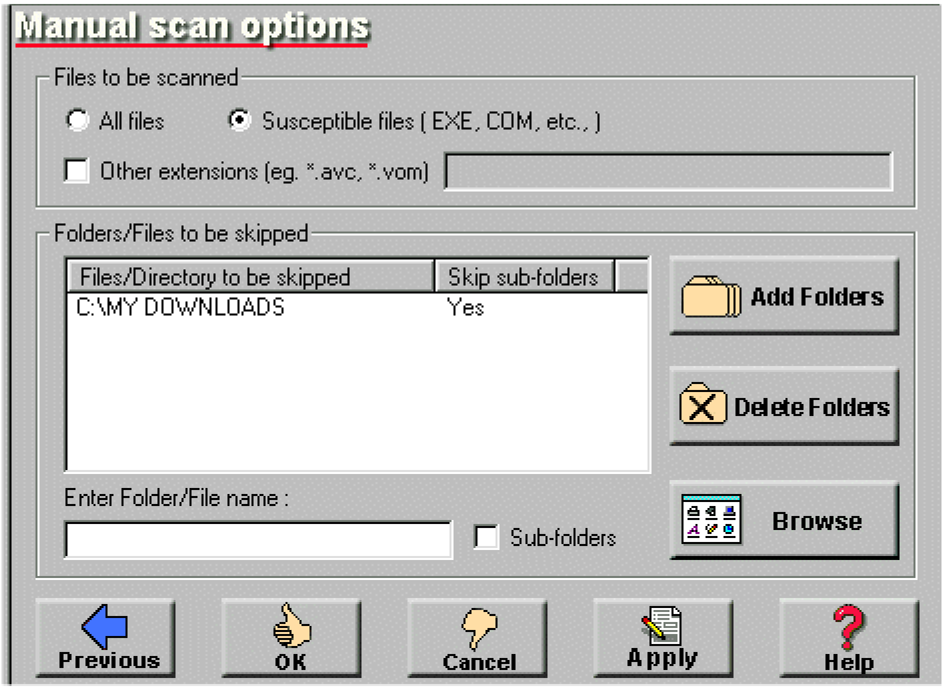
1. Enable the Other Extensions switch, by right clicking the mouse button. In the box, enter the extension to be scanned. Standard wildcards, like *.VOM, AB*.EXE, etc., are accepted.
2. Once you have completed entering the file extensions you want scanned for virus, click on the OK button to save and exit. Clicking on the Apply button will save the settings only for the current session.

Folders/Files to be skipped

Folders or Files that are added to this list are not checked for viruses by the Scanner. To stop the Scanner from checking a file for virus, follow these steps.

1. Go to Folders/Files to be Skipped. In the field that says Enter Folder/File name, type the name of the file that is not to be checked, along with the path. Click on the Add Folders button. The extension is displayed in the main window. Alternatively, you can also browse and pick up the file you want added by clicking on the Browse button. Standard wildcards, like *.VOM, AB*.EXE, etc., are accepted.
2. If the path terminates in a folder, then the entire folder is not checked for virus. Under each folder, sub-folders can be checked or skipped by the Scanner depending on whether the Sub-folder option is disabled or enabled. them
3. If the session is done, click on the OK button to save and exit. Clicking on the Apply button will save the settings only for the current session.

It is recommended that this feature be used with extreme caution. Files that are to be skipped will not be scanned for viruses.



Manual scan options

Files to be scanned

○ All files ● Susceptible files (EXE, COM, etc.,)

□ Other extensions (eg. *.avc, *.vom)

Folders/Files to be skipped

Files/Directory to be skipped	Skip sub-folders
C:\MY DOWNLOADS	Yes

Enter Folder/File name :

□ Sub-folders

All accessed files are checked for virus by the real-time scanner, when this option is enabled.

Only those files that are susceptible to virus are checked when this option is enabled. See detailed help for a list of susceptible files.

Specific file extensions can be added to the scan list , in addition to the susceptible files that are always checked by default. Enable the Other Extensions switch, by right clicking the mouse button. In the box, enter the extension to be scanned. Standard wildcards, like *.VOM, AB*.EXE, etc., are accepted.

Folders or Files that are added to this list are not checked for viruses by the Scanner. To stop the Scanner from checking a file for virus, follow these steps.

In the field that says Enter Folder/File name, type the name of the file that is not to be checked, along with the path. Click on the Add Folders button. The extension is displayed in the main window. Alternatively, you can also browse and pick up the file you want added by clicking on the Browse button. Standard wildcards, like *.VOM, AB*.EXE, etc., are accepted.

If the path terminates in a folder, then the entire folder is not checked for virus. Under each folder, sub-folders can be checked or skipped by the Scanner depending on whether the Sub-folder option is disabled or enabled.

Folders or Files that are added to this list are not checked for viruses by the Scanner. To stop the Scanner from checking a file for virus

The scanner can automatically disinfect the file. Only one course of action can be selected.

The scanner can automatically delete the file. Only one course of action can be selected.

Protector Plus will check for viruses in memory whenever a Manual Scan is invoked. If viruses are found in the memory, they are de-activated.

The scanner can automatically rename the file. Only one course of action can be selected.

The scanner can automatically quarantine the file. Infected file will be moved to the quarantine directory. Only one course of action can be selected.

The scanner will ignore the file. Only one course of action can be selected.

The scanner will deny access to the infected file.

Viewing Real-time Scan Report

Each time the Real Time Scanner or the Email Scanner detects a virus,   a report is generated. This report contains the following information; name of the infected file, name of the virus found, time the infection was detected and the action taken by the Real Time Scanner. If the virus is detected by the Email Scanner, it also lists the sender's name in addition to the above information.

A history of such reports can be maintained. By default, the file is stored under Protector Plus installed directory. The default size limit is 1000k. The name of the report file and it's size can both be altered.

Find:

The scan report can be searched for specific characters or words. Enter the characters or words that you would like to find in the window displayed.

Print:

The scan report can be printed as displayed.

Viewing Manual Scan Report

There are two kinds of Manual Scan Reports. One report furnishes details of the last manual scan performed and the other is a consolidated report of all manual scans done till date.

Last Scan Report

The Last Scan Report contains details of time when the last scan was performed, the file that was infected, name of the virus that was causing infection, and the action taken by Protector Plus.

Scan History

Details of the results of all scans performed by the Manual Scanner are displayed when Scan History is clicked. Details include consolidated information on when the manual scan was performed, the file that was infected, name of the virus that was causing infection, and the action taken by Protector Plus

Please note that a report is generated only in the event that a virus is found by the Scanner. In case there is no virus infection, then no report is generated.

InstaUpdate

InstaUpdate ensures that the version of Protector Plus installed on a computer is always current. It compares the version on the web site with the one installed on the computer. If the version on the web site has been upgraded, then InstaUpdate automatically downloads and installs the upgrade on the computer.

Download Update

InstaUpdate can be configured to download and install updates only if the Download Update option is enabled.

Prompt before Downloading

If this box is enabled, then InstaUpdate will ask the user for a prompt before going ahead with the download. If not, the process takes place in the background, without requesting for the user's permission.

Frequency

InstaUpdate will connect to the web site at pre-configured frequencies to check for upgrades. The frequency is set in either months or days.

There are two kinds of upgrades, one Product upgrades, and two, virus database upgrades. Product upgrades happen infrequently, on an average, six times a year. Therefore it is recommended that InstaUpdate checks the web site for Product Upgrades once in a month.

Virus Database Upgrades are more frequent, and therefore InstaUpdate should be configured to check the web site once in a week or two at the maximum.

Connect Now

InstaUpdate can be forced to connect to the web site and check for upgrades at any point in time, by clicking on the, 'Connect Now' button. Forcing a connection overrides the frequency options that are configured.

Internet address at which upgrades are available

By default, the Internet address of the web site where upgrades are released is **Error! Reference source not found.** . However, alternate sites can be entered if upgrades are known to be available from there.

Upgrading from a PPCD server

Where Protector Plus Console for Desktops (more information available at **Error! Reference source not found.**) is installed, InstaUpdate will pick up upgrades from the PPCD server and install them onto the computer.

Enter the name of the folder in which the upgrades are available in the box provided under, 'Download upgrades from a local (PPCD) server'. InstaUpdate will constantly check this folder for the presence of upgrades.

Saving Configurations

Once the selections have been made, clicking on the OK button saves the settings, clicking on APPLY saves the settings only for the current session, and CANCEL, discards the changes made and returns the system to it's previous state.

InstaUpdate can be configured to download and install updates only if the Download Update option is enabled.

If this box is enabled, then InstaUpdate will ask the user for a prompt before going ahead with the download. If not, the process takes place in the background, without requesting for the user's permission.

InstaUpdate will connect to the web site at pre-configured frequencies to check for upgrades.   The frequency is set in either months or days.

There are two kinds of upgrades, one Product upgrades, and two, virus database upgrades. Product upgrades happen infrequently, on an average, six times a year. Therefore it is recommended that InstaUpdate checks the web site for Product Upgrades once in a month.

Virus Database Upgrades are more frequent, and therefore InstaUpdate should be configured to check the web site once in a week or two at the maximum.

InstaUpdate can be forced to connect to the web site and check for upgrades at any point in time, by clicking on the, 'Connect Now' button. Forcing a connection overrides the frequency options that are configured.

By default, the Internet address of the web site where upgrades are released is **Error! Reference source not found.** .   However, alternate sites can be entered if upgrades are known to be available from there.

Where Protector Plus Console for Desktops (more information available at **Error! Reference source not found.**) is installed, InstaUpdate will pick up upgrades from the PPCD server and install them onto the computer.

Enter the name of the folder in which the upgrades are available in the box provided under, 'Download upgrades from a local (PPCD) server'. InstaUpdate will constantly check this folder for the presence of upgrades.

Once the selections have been made, clicking on the OK button saves the settings, clicking on APPLY saves the settings only for the current session, and CANCEL, discards the changes made and returns the system to it's previous state.

Quarantine

When an infected or suspect file cannot be cleaned by the Real-time or Manual scanner, it can be moved to a Quarantine directory. The quarantine directory is created under the root directory.

Files in the Quarantine directory can be deleted, cleaned and/or moved back to their original directory. Files can reside in the Quarantine directory till such time that upgrades to clean them are supplied by us. If the object restored from the quarantine is an email attachment, it will be re-sent to your mailbox by Protector Plus. It will appear as new email when you download your email next time.

Quarantine Status

Qurantine Status indicates the directory path and the number of files currently in quarantine.

Quarantine Information

Last Quarantine Date/Time : Displays the date and time when the last infected file was moved to the Quarantine directory

Virus Database Version : Indicates the virus database version of Protector Plus when the last move to the quarantine directory was effected.

Product Version : Indicates the product version of Protector Plus when the last move to the Quarantine directory was effected.

Current Product Information

Displays the current version of Protector Plus.

Origin of file

Displays the path from where the quarantined file was moved. Additional information given are the date and time when the file was moved, and the name of virus infecting the file.

Deleting a file(s) in the Quarantine directory

Select the file(s) that is(are) to be deleted by clicking on the file with the left mouse button. Go to Delete button at the bottom of the menu and click on it to delete file.

Scanning a file(s) in the Quarantine directory

Select the file(s) that is(are) to be scanned from the list displayed in the Quarantine window. Go to the Scan button at the bottom of the menu and click on it to initiate the Manual Scan. Whatever options are set in the Manual Scan are displayed when the virus is encountered. Select the option suited to your requirements.

Restoring a file to it's original location

After a file has been scanned and cleaned of the virus, it can be moved back to it's original location. Select the file that is to be moved back, and click on the Restore button at the bottom of the menu. The file is automatically moved to it's original location.

Quitting the Qurantine menu

Click on Cancel to exit the Quarantine menu.

Qurantine Status indicates the directory path and the number of files currently in quarantine.

Last Quarantine Date/Time : Displays the date and time when the last infected file was moved to the Quarantine directory

Virus Database Version : Indicates the virus database version of Protector Plus when the last move to the quarantine directory was effected.

Product Version : Indicates the product version of Protector Plus when the last move to the Quarantine directory was effected.

Displays the current version of Protector Plus.

Displays the path from where the quarantined file was moved. Additional information given are the date and time when the file was moved, and the name of virus infecting the file.

Select the file(s) that is(are) to be deleted by clicking on the file with the left mouse button.
Go to Delete button at the bottom of the menu and click on it to delete file.

Select the file(s) that is(are) to be scanned from the list displayed in the Quarantine window.
Go to the Scan button at the bottom of the menu and click on it to initiate the Manual Scan.
Whatever options are set in the Manual Scan are displayed when the virus is encountered.
Select the option suited to your requirements.

After a file has been scanned and cleaned of the virus, it can be moved back to it's original location. Select the file that is to be moved back, and click on the Restore button at the bottom of the menu. The file is automatically moved to it's original location.

Click on Cancel to exit the Quarantine menu.

Real-time Scan Status

On-line status gives statistics related to the Real-time scanner's current activities. The scanning window displays the file currently being scanned for virus.

Real-time scan statistics

Real-time scan statistics display the total number of files scanned by the Real-time scanner, the number of files that were infected, and the number of those infected files that were disinfected, deleted, renamed or quarantined.

The main window displays the name of the file that is infected, by which virus and the action taken. Click on the OK button to exit the screen.

Rescue Disk

The rescue disk contains critical system information that is useful in restoring a computer to a normal state should it become unbootable for some reason.

The main menu displays the Rescue Disk status. The name of the computer, whether or not a Rescue Disk has been created on the computer, and the version of Protector Plus that was running when the Rescue Disk was created are shown.

Creating a rescue disk

It is advisable to start with a fresh disk when creating a rescue disk.

1. Insert the disk in the floppy drive and click on the Create Disk button.
2. A pop-up box asks you to give the Rescue Disk a name. The length of the name can be between 1 and 128 characters.
3. Click on the OK button in the pop-up menu after entering a name.
4. The Rescue Disk will have to be formatted before the computer's data is written onto it. The formatting is done by the Windows' Format program.
5. Click on the OK button in the dialog box. You are now taken to the Windows', 'Format', program.
6. The default selection of the Format program is 1.44 Mb floppy and the Format type is, 'Full'.
7. Click on the 'Start' button, to commence formatting.
8. Once the format operation is over, click on the, 'Close' button, in the dialog box that is displayed.
9. You are returned to the Format program window. Click on the, 'Close' button to finish the Format operation.
10. Once the format operation is over, critical system information and some Protector Plus files are written onto the Rescue Disk.
11. Click on the ok button in the dialog box that informs you that the process of creating the Rescue Disk is completed.
12. Label the Rescue Disk as such and preserve it in a safe place.
13. The main menu of the Rescue Disk now displays the name of the computer as known to the Rescue Disk, the date on which it was created and the version of Protector Plus that was copied onto it.

Verifying the Rescue Disk

The verification process checks for two things;

1. Whether or not the disk inserted was created on that computer as a Rescue Disk.
2. For the integrity of the information stored on it.

If the verification process fails on any one of these two counts, create a fresh Rescue Disk.

Scan Selected Folders

A single or a set of folders can be checked for virus at any time. To check a single folder or a set of folders,

1. Click on the Scan Selected Folders option.
2. In the browser window that appears, tick the folders you want checked for viruses.
3. Click on the Scan button at the bottom of the browser window to detect viruses in the selected folders.

To Scan all folders except one (or a few).

1. Click on the Scan Selected Folders option.
2. In the browser window that is displayed,   double click on the folder or the + button to expand the folder tree.
3. Tick the small box next to the folder you want scanned. All the sub folders under it are also automatically selected for scanning.
4. Under the selected folder, go to the folder(s) you do not want checked and unselect it, by clicking on the box adjacent to the folder name.
5. Lastly, click on the Scan button at the bottom of the browser window and all the selected folders are scanned for virus.

In the browser window that appears, go to the file to be scanned. Double click on the file or click on the Open button and the file will be checked for virus.

Reports

To view different types of reports.

You can view different types of reports using these options.

1. Real-time Scan Report.
2. Manual Scan Report.

Manual Scan Report

Each time the Manual Scanner detects a virus,   a report is generated. This report contains the following information; name of the infected file, name of the virus found, time the infection was detected and the action taken by the Manual Scanner.

A history of such reports can be maintained. By default, the file is stored under Protector Plus installed directory. The default size limit is 1000k. The name of the report file and it's size can both can be altered.

Find:

The scan report can be searched for specific characters or words. Enter the characters or words that you would like to find in the window displayed.

Print:

The scan report can be printed as displayed.

Help is not Available

Protector Plus help is not available for this particular topic. You can return to Main help window for further topics.

Registration

To Register and legalize the use of Protector Plus, Please enter the **Name** and **Registration key** in the Register window by choosing the Register Now option. The Registration key supplied by us is unique to the Name to which this software is registered. Typing ERRORS in either field will result in failure of registration.

Obtaining Registration Key :

Please visit
http://www.protectorplus.com/order/order.htm
to understand the registration process. To get the registration key, you have to pay us the requisite fees. On receiving the fees, we will supply you with the Registration key within two working days. Please note that all the correspondence and communication will be through Email.

Email : sales@protectorplus.com
Internet: http://www.protectorplus.com

How to Register :

1. You can only register this copy of the software through the web.

2. The registration fees are accepted only when made through credit card. Our collection agent will accept payments made in US dollars only.

3. Pricing details are available at
http://www.protectorplus.com/register/prices.htm
Discounts are available for multiple copy purchases.

4. To register the software in your name, or the name of your choice, go to
http://www.protectorplus.com/order/order.htm
and submit your order for processing.

You will need to have the following details in hand.

Name : The person or organization you want the software registered to.

Email address : Of the person or organization you want the software registered to.

Postal address : Of the person or organization you want the software registered to.

Your credit card number : The credit card number from which you are making the purchase, along with expiry date.

The products and the number of copies that you want to order.

Fill out the order form and submit it to us for processing. You will receive an acknowledgement from our payment collection agent within 48 hours of submitting the order. Within two working days we will dispatch a **Registration key**.

On receiving the **Registration key**, please go to the **Register** option in the demo pack you have downloaded. In the dialog box that appears, fill in the following details

Name : Key in the same name that you have sent to us for registering the software.

Registration key : Enter the Key sent by us.

Please note that the Name and Key should match what has been sent by us. Otherwise, it will result in a failure of the registration.

What you get on registering.

1. You will become a licensed user of Protector Plus.

2. You will be entitled to regular upgrades that we release. Your Email address will be added to our mailing list and you will be notified as and when releases are made.

3. The prompts that appear asking you to register the software each time a viral activity is detected and tackled by the evaluation pack will subside.

4. Please note that support will only be through the Internet.

Registration Error

This error will occur when the registration Name and Key do not   match. Please check for the name and registration key typed properly or not.

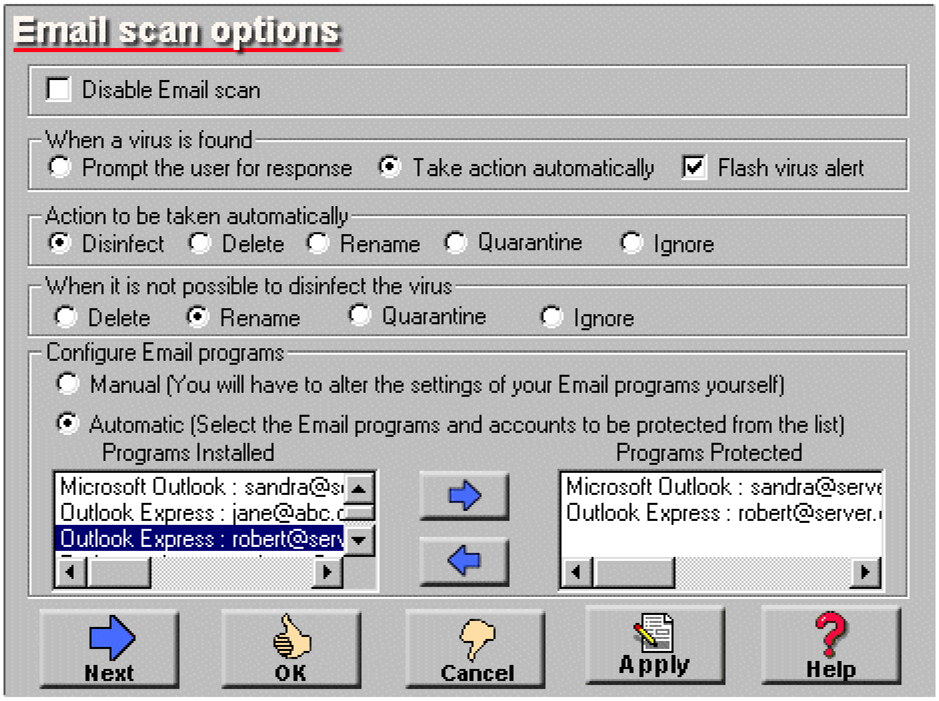
If not, obtain a Registration key for the Name you want the software to be registered.

How to Register

Email Scan

Protector Plus detects viruses present in infected Emails before they are dowloaded on to the computer. In addition to detecting the viruses, the Email Scan can also inform the sender of the infected mail that the mail sent was infected with a virus.

Click on the topic to view the context sensitive on-line help.



Email scan options

☐ Disable Email scan

When a virus is found
○ Prompt the user for response ● Take action automatically ☑ Flash virus alert

Action to be taken automatically
● Disinfect ○ Delete ○ Rename ○ Quarantine ○ Ignore

When it is not possible to disinfect the virus
○ Delete ● Rename ○ Quarantine ○ Ignore

Configure Email programs
○ Manual (You will have to alter the settings of your Email programs yourself)
● Automatic (Select the Email programs and accounts to be protected from the list)

Programs Installed	Programs Protected
Microsoft Outlook : sandra@s	Microsoft Outlook : sandra@serve
Outlook Express : jane@abc.c	Outlook Express : robert@server.
Outlook Express : robert@serv	

Click on the checkbox to enable or disable the Email scan. If the switch is enabled, then Protector Plus will not check the incoming Email messages for viruses.

Configure Email Programs

The Email Scan feature can be applied selectively to Email programs installed in the computer.

Protector Plus will list all the Email programs installed in the computer, in the **Programs Installed** window. For Protector Plus to scan Emails downloaded through a particular program, click on the program in the **Programs Installed** window, and then click on the right arrow. The selected program will appear in the **Programs Protected** window. All Emails downloaded through programs listed in the **Programs Protected** window will be checked for viruses.

If it is required to configure an Email program not listed in the Programs Listed menu, you can choose **Manual** option and configure manually. Please visit the link for instructions on configuring the program.

http://www.protectorplus.com/products/features/emconf.htm

Renewal

The license to download Protector Plus virus database and product (engine) updates is valid for 12 months from the date of purchase. It is now over 12 months since this copy of Protector Plus was purchased and consequently, the license to download updates has lapsed. To renew this license please visit:

http://www.protectorplus.com/order/renewal.htm

If you have any problems with regard to renewal that you would like us to address, please fill out the on-line form available at

http://www.protectorplus.com/support/renforum.htm

Our Customer Relations Center will revert to you as soon as possible.

If you require any further information, please write to **sales@protectorplus.com.**

Alerts can be sent to a list of email addresses whenever Protector Plus detects a virus in an email. Click on the checkbox to enable others to receive these alerts.

Enter the email addresses that should be alerted when Protector Plus detects a virus in an email. Click the, "Add" button to add the email address to the alert list. To remove an address from the alert list, select the email address to be removed and click the, "Remove" button.

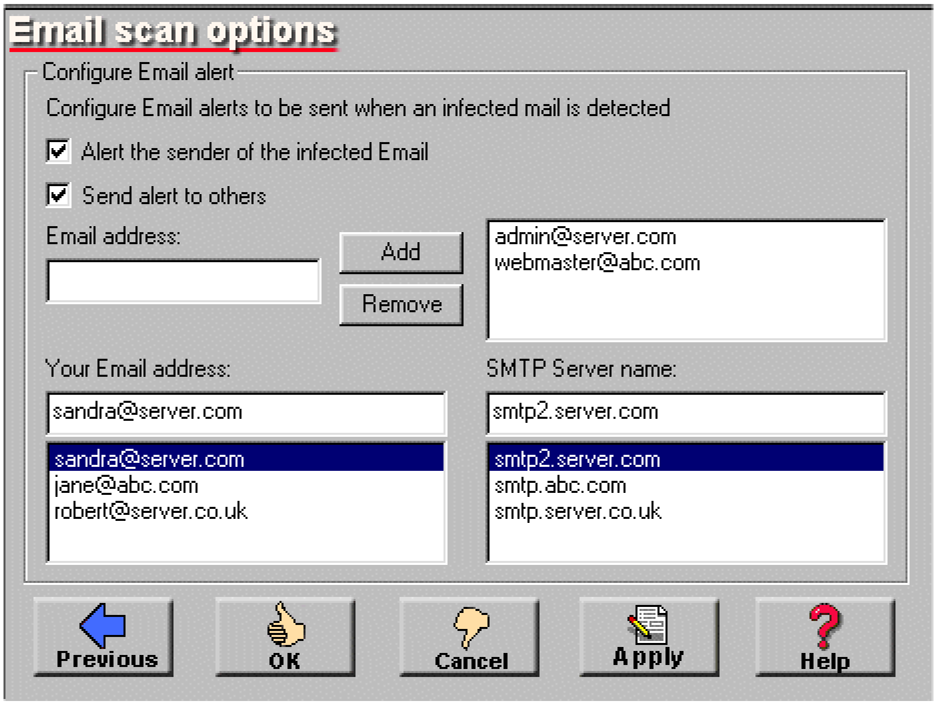
Enter your email address here. The alert email message will have this email address as the "From" address.

Enter your SMTP server name or select from the list displayed. Protector Plus will use this server to send the alert message when it detects a virus.

Email Alerts

Protector Plus can be configured to send an email alert when an infected mail is detected. The alert can be sent to the email address from where the infected email originated. Similar alerts can be sent to others. This list can be configured.

Click on the topic to view the context sensitive on-line help.



Email scan options

Configure Email alert

Configure Email alerts to be sent when an infected mail is detected

☑ Alert the sender of the infected Email

☑ Send alert to others

Email address:

admin@server.com
webmaster@abc.com

Your Email address: sandra@server.com

sandra@server.com
jane@abc.com
robert@server.co.uk

SMTP Server name: smtp2.server.com

smtp2.server.com
smtp.abc.com
smtp.server.co.uk

Protector Plus can alert senders of infected mail messages that they have sent viruses by email. Click on the checkbox to enable or disable this alert.

Renewal Error

This error will occur when the renewal registration Key do not match with the Registered Name. Please check for the registration key typed properly or not.

If not, obtain a Renewal Registration key in the Name you have registered earlier.

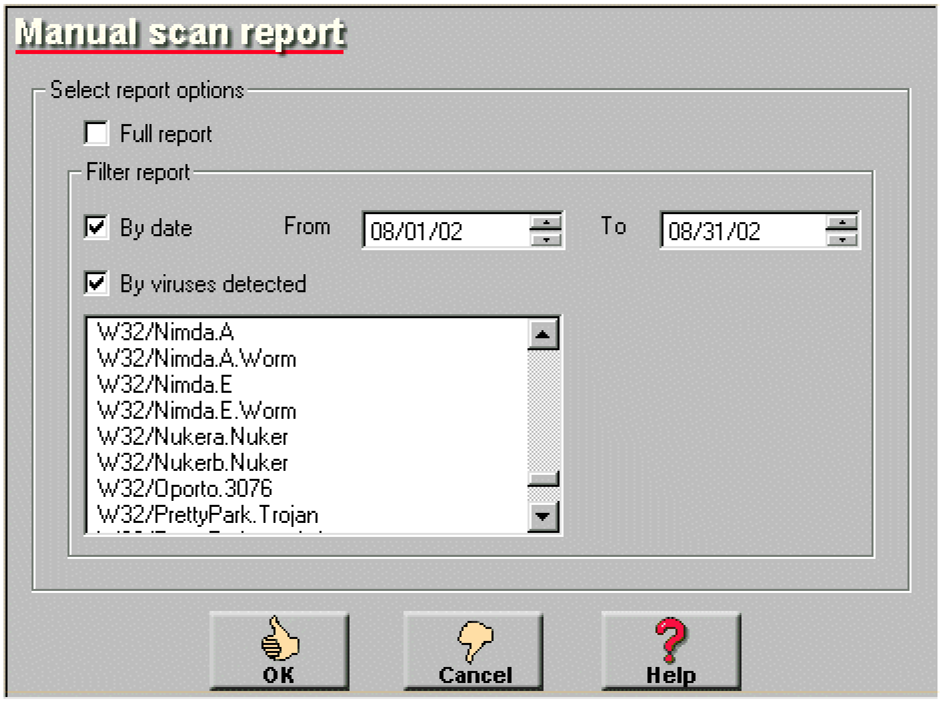
How to Renew

Protector Plus can instantly scan any file that is accessed through Explorer, by right-click. The scanner can be accessed at any point through a single click, saving the user time and giving greater flexibility in the use of Protector Plus.

Manual Scan Report

Reports are generated that will help the user understand the origin of virus activities in the computer. The knowledge can be useful in preventing virus infections from the same or similar source.

Click on the topic to view the context sensitive on-line help.



Manual scan report

Select report options

☐ Full report

Filter report

☑ By date From 08/01/02 To 08/31/02

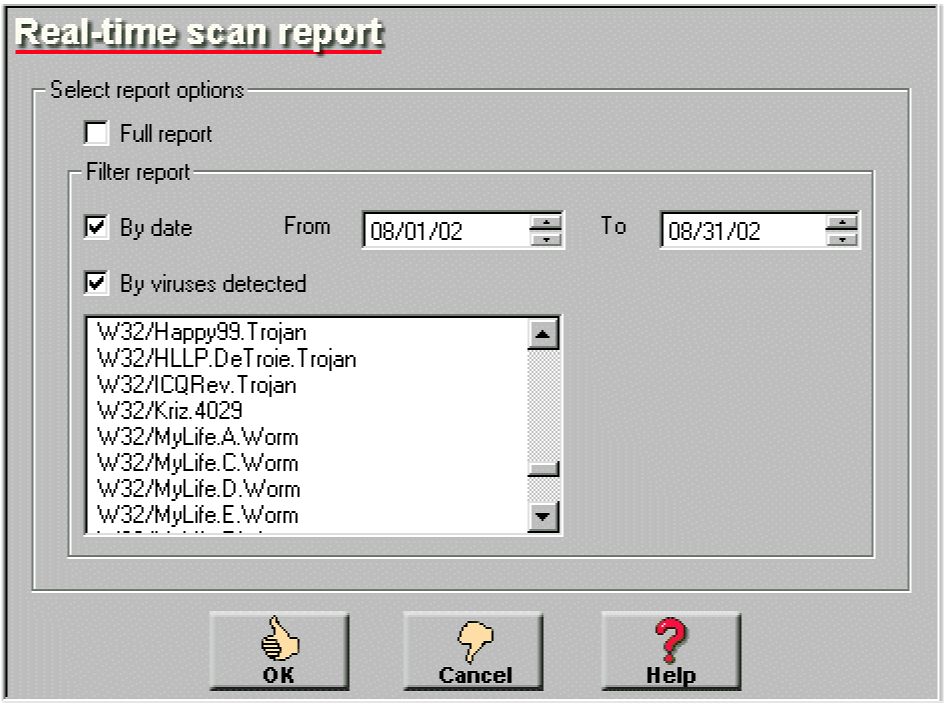
☑ By viruses detected

W32/Nimda.A
W32/Nimda.A.Worm
W32/Nimda.E
W32/Nimda.E.Worm
W32/Nukera.Nuker
W32/Nukerb.Nuker
W32/Oporto.3076
W32/PrettyPark.Trojan

Real-time Scan Report

Reports are generated that will help the user understand the origin of virus activities in the computer. The knowledge can be useful in preventing virus infections from the same or similar source.

Click on the topic to view the context sensitive on-line help.



Real-time scan report

Select report options

□ Full report

Filter report

☑ By date From 08/01/02 To 08/31/02

☑ By viruses detected

W32/Happy99.Trojan
W32/HLLP.DeTroie.Trojan
W32/ICQRev.Trojan
W32/Kriz.4029
W32/MyLife.A.Worm
W32/MyLife.C.Worm
W32/MyLife.D.Worm
W32/MyLife.E.Worm

Displays the complete report.

Generates and displays a report of all viruses detected between the selected dates.

A report listing the activities of the viruses detected by Protector Plus can be generated. The report can be for an individual virus or a combination of viruses.