Adds a notification alert recipient.

Removes the selected alert notification item.

Configures the selected item.

Lists the currently configured systems to receive notification alerts.

Tests the alert notification.

Enter the pager number of the alert notification recipient.

Opens a Browse dialog box. Search for a system to receive notifications.

Opens the Modem Configuration dialog box.

Opens the SMTP (Simple Mail Transfer Protocol) configuration dialog box.

Specify the server to use.

Opens a Browse dialog box. Search for a printer to receive notifications.

Enter the Login name for the server.

When enabled, the system sends standard alert messages.

When enabled, the system sends the custom alert message.

Enter the amount of time to elapse between dialing the phone number and entering the numeric message.

Enter the pager ID number or PIN number (if applicable).

Enter the pager password (if applicable).

Enables sending alerts via SNMP (Simple Network Management Protocol).

Turns the modem speaker off.

Use the up or down arrows to increase or decrease the value in this spin box.

Select the priority level configuration to use.

No text associated with this topic. .

Enables SNMP. Refer to Windows NT documentation for more information.

Configures SNMP. Refer to Windows NT documentation for more information.

Enter the brand of modem. If your modem is not listed, select a generic modem.

Enter a custom alphanumeric message.

Enter the amount of time to elapse between dialing the phone number and sending the numeric message.

Enter the modem's maximum baud rate.

Select the type of pager to receive notifications.

Enter the name of the message sender.

Enter the pager ID number or PIN number (if applicable).

Enter the pager password (if applicable).

Enter an E-mail Subject line.

Enter any prefix required to get an outside line (eg: 9). Insert a comma(s) to create a two second delay in dialing.

Enter any necessary suffix (eg: password).

Enter the COM port to which the modem is attached.

Selects Tone dialing.

Selects Pulse dialing.

Enter the file to be executed.

Enter the name and path of the program to execute as a means of alert notification.

Instructs the system to run the program only for the first alert.

Instructs the system to run the program for every alert.

Instructs the system to log system alert notifications to the server specified below.

Instructs the system to execute a program as a means of alert notification.

Enter the maximum log file size.

Specify the screen refresh frequency in the provided spin box.

Choose a computer to receive event log notification.

Instructs the system to send alerts to the Alert Manager.

Select this checkbox to send alerts to the Alert Manager. Then, click the Configure button to configure the Alert Manager settings.

Enter the day of the month to start this task.

Enter the item to add. Drives, folders, or files may be specified.

Select an item by browsing current drives, folders, and files.

Instructs AutoUpdate to store the update package in a particular location. Other computers can point to this location for updates.

Select the location where the update package is stored. Other computers may point to this location for updates.

Instructs AutoUpdate to copy an update package from a path or UNC location.

Save new DAT files without applying them. Enter a location where the update package will be saved.

Instructs AutoUpdate to retrieve the update package from an FTP location.

Instructs AutoUpdate to retrieve the update or upgrade package now.

Enable this option to instruct the on-access scanner to maintain a virus log file. Enter a name and path for the log file in the text box below.

Enables logging to the log file. The log file keeps a record of virus activity.

Enter a name and location for the log file.

Opens a Browse dialog box. Choose a log file location.

Limits the log file size. Deselect this option for unlimited log file size.

Creates a log entry when a virus is detected.

Creates a log entry when a virus is cleaned.

Creates a log entry when a virus is deleted.

Creates a log entry specifying the session settings.

Creates a log entry summarizing the scan session.

Appends the date and time to each log entry.

Appends the user name to each log entry.

Instructs the scanner to search for viruses inside all file types.

Instructs the scanner to search for viruses inside files with specific extensions (specified by clicking the File Types button).

Displays items to exclude from scanning.

Adds exclusion items.

Specifies the action the VirusScan takes when a virus is encountered.

Removes the highlighted exclusion item.

Edits the highlighted exclusion item.

Enter the item to exclude. Drives, folders, or files may be specified.

Allows users to disable VirusScan scan tasks.

Resets the program file extensions list to the default setting.

Enter a new file extension.

Enter the location to quarantine infected files.

Select the folder to quarantine infected files.

Opens the Program File Extensions dialog box. From this dialog box, you can specify the types of files VirusScan checks.

Instructs the on-access scanner to scan files compressed with PKLite and LZEXE.

Displays program file extensions.

Enable this option to scan inbound files.

Adds a file extension.

Enable this option to scan outbound files.

Deletes an extension.

Opens a Browse dialog box. Search for a folder to exclude.

Excludes subfolders from scanning.

Excludes the item from inbound scanning.

Excludes the item from outbound scanning.

Activates the McAfee TaskManager at system startup.

Browse to locate the file.

Displays scanning locations (local drives, network drives, folders) as items. Scan items may be added, edited, or deleted.

Adds a scan item.

Removes the selected scan item.

Edits the selected scan item.

Instructs VirusScan to search for viruses in all subfolders.

Instructs VirusScan to display a custom message upon virus detection (the Action option must be set to Prompt for action).

Instructs VirusScan to sound an alert upon virus detection (the Action option must be set to Prompt for action). The alert sounds at the end of scan.

Enable this option to instruct VirusScan to maintain a virus log file.

Enter a name and path for the log file.

Limits the maximum size of the log file. Deselect this option for unlimited log file size.

Enter the maximum log file size.

Instructs the scheduler to run this task once at the time specified in the ‘Start at’ field.

Instructs the scheduler to run this task hourly at the time specified in the ‘Start at’ field.

Instructs the scheduler to run this task daily at the time specified in the ‘Start at’ field. To specify the days the scheduler runs, click the Which Days button.

Specifies which day(s) of the week the scheduler will run this task.
The Daily radio button must be selected to use this feature.

Instructs the scheduler to run this task weekly at the time and day specified in the ‘Start at’ field.

Instructs the scheduler to run this task monthly at the time and day specified in the ‘Start at’ field.

Instructs the scheduler to transparently run this task when the McAfee Task Manager service is started.

Enter the month to start the task.

Enter the day to start this task.

Enter the day to start this task.

Enables the scheduler for this task.

Enter the start time for this task.

Enter the date to start this task.

Instructs VirusScan to search for viruses inside files compressed with PKZIP, PkLite, LHA, LZEXE and Microsoft CAB.

Enter the number of minutes after the hour to start the hourly task.

Enter the start time for this task.

Enter the start time for this task.

Enter the start time for this task.

Enter the start time for this task.

Enter the start time for this task.

Instructs VirusScan to create a log entry when a virus is detected.

Instructs VirusScan to create a log entry when a virus is cleaned.

Instructs VirusScan to create a log entry when a virus is deleted.

Instructs VirusScan to create a log entry when a virus is moved.

Instructs VirusScan to create a log entry specifying the session settings.

Instructs VirusScan to create a log entry summarizing the session.

Instructs VirusScan to append the date and time to each log entry.

Instructs VirusScan to append the user name to each log entry.

Select an item to add to the scan.

Select this option to scan the specified items immediately without saving the task.

Check this option to skip boot record scanning

Check this option to skip memory scanning.

Displays the Advanced Scanner Settings screen.

Use this screen to set the priority of this task and to skip scanning of the boot record.

Select this option to save the current settings as a task and exit without scanning.

Enter the desired name for this task.

Allows you to assign a name to the newly created task.

Displays the names and characteristics of known viruses from McAfee's virus definitions file. This list can be sorted by clicking a column title.

Indicates the virus is memory resident.

Indicates the virus is encrypted.

Indicates the virus is a polymorphic virus.

Check this box to enable Centralized Alerting for this server. The server will be able to receive alerts from McAfee workstation antivirus products and perform activity logging, event logging and alerting as defined for this server.

Indicates the virus has a remover available.

Logs alerts in the local computer's application log.

Logs alerts in another computer's application.

Creates a log entry when a virus is moved to the ‘‘quarantine’’ directory.

Removes the remote users permissions from the network share when a virus is detected.

Enables the Intelligent Caching feature to significantly improve on-access scanning performance. When this option is enabled, the on-access scanner will only scan files the first time they are accessed after the system or Task Manager is restarted. If a file in the cache is modified, the on-access scanner rescans the file.

Scans floppy disks left in the disk drive before system shutdown.

Scan mapped or UNC network drives.

Browse to locate the folder.

No text associated with this topic

Enter the server name and login name of the receiving account.

Enables you to select a method for error checking.

Enter a custom message.

Enable DMI alerting to send virus notifications to the Management Interface from DMI-enabled computers.

Notify user of virus. Enter your custom message in the text box below.

Browse to locate the folder.

Selecting this option will save the current settings as a task, then run the task.

Browse to locate the computer name and directory.

Select this option to use an anonymous FTP login. If this option is selected, AutoUpdate will automatically assign ‘‘Anonymous’’ as your user name and assign your e-mail address as your password.

Enter login name and password.

Select this checkbox if your environment requires that you use a proxy server to access the Internet via FTP.

Enter the port number of the proxy server.

Enter the name of the proxy server.

Record all AutoUpdate activity.

Schedule AutoUpdate tasks.

Configure additional AutoUpdate options.

Save the files without applying them. Enable this option on the local network computer that other computers will copy the update packages from.

Save the files to a special location without applying them.

Browse to the location where the upgrade package will be saved.

Save the existing DAT files.

Save the files to a special location without applying them.

Browse to the location where the update package will be saved.

Automatically execute a program or script upon updating the DAT files.

Locate the file to run.

Enter your user name.

Enter a password.

Reenter the password above.

Creates a log entry summarizing the scan session.

Select this option to save and run the current settings as a task.

Browse to select a directory for Centralized Alerting.

Opens the Browse dialog box. Choose a location to quarantine the infected file.

Browse to locate the folder.

Select this option to automatically start scanning each time the computer is started.

Brings up a Browse dialog box. Browse to locate the program.

Enter the name of the computer to receive alert notifications.

Enter the full e-mail address of the alert message recipient.

Enter the name of the printer that will receive printed alerts. Include the computer name and path of the printer.

Enter a numeric message.

Sound an audible alert upon virus detection.

Enter the full path to a sound file to play upon virus detection.

Opens the Browse dialog box. Search for a sound file to use for alerts.

Instructs the system to execute a program as a means of alert notification.

Enter the full path of a program to be run upon alert notification.

“Migrated files” are infected files that VirusScan moved to a “quarantine” area. Select this option to exclude “quarantined” files from scanning.