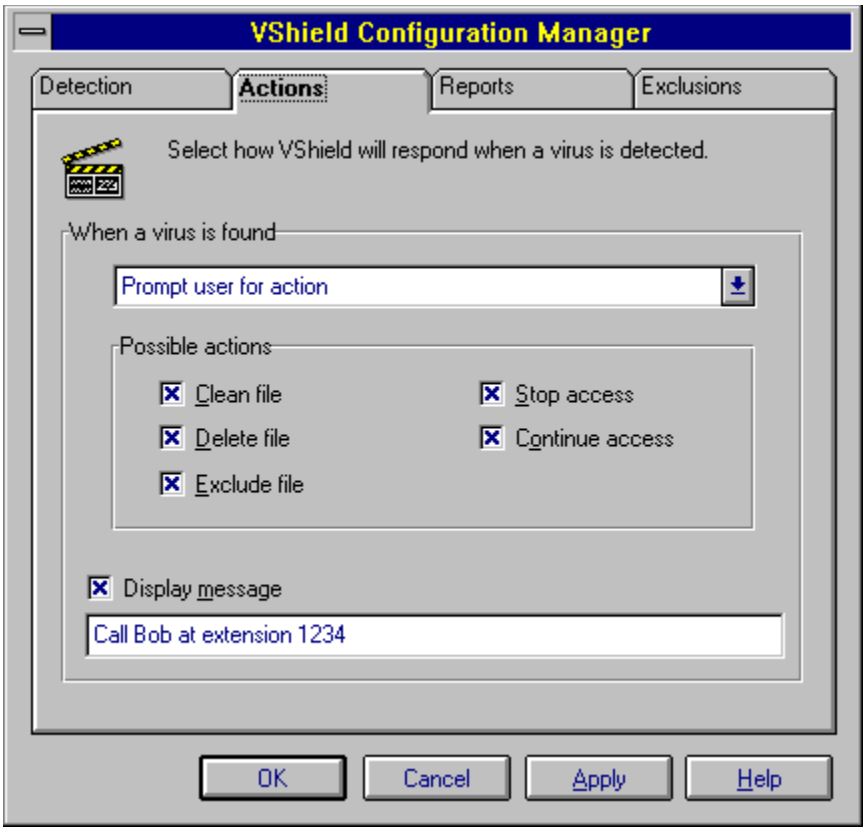

VShield Configuration Manager
Detection
Actions
Reports
Exclusions
Use this page to identify what will be scanned and when scanning will take place.
Scan files on
Run
Create
Copy
Rename
Scan disks on
Access
What to scan
All files
Compressed files
Program files only
Program Files...
General
Load VShield at startup
VShield can be disabled
Show icon on the desktop
OK
Cancel
Apply
Help


VShield Configuration Manager
Detection
Actions
Reports
Exclusions
Select how VShield will respond when a virus is detected.
When a virus is found
Prompt user for action
Possible actions
Clean file
Delete file
Exclude file
Stop access
Continue access
Display message
Call Bob at extension 1234
OK
Cancel
Apply
Help


VShield Configuration Manager
Detection
Actions
Reports
Exclusions
Configure the logging of virus activity. Define what information will be captured for each log entry.
Log file
Log to file:
d:\actilog.txt
Browse...
Limit size of log file to:
100
kilobytes
What to log
Virus detection
Virus cleaning
Infected file deletion
Infected file move
Session settings
Session summary
Date and time
OK
Cancel
Apply
Help

Selecting this option instructs VShield to scan for viruses inside all files. Selecting this option provides optimal protection.

Selecting this option instructs VShield to only scan for viruses inside program files. This option allows the user to customize VShield for performance without sacrificing protection.

Selecting this option instructs VShield to scan for viruses in executable files compressed with PkLite and LZEXE.

Click this to specify program file extensions.

Use this field to specify the action to be taken when a virus is detected.

Selecting this option instructs VShield to display a custom message upon virus detection. For the message to be displayed, the Action option above must be set to **Prompt for action**.

Enter the desired message to be displayed upon virus detection.

Selecting this option instructs VShield to log information to the specified log file.

Enter the desired log file in the provided text box.

Selecting this option instructs VShield to create and maintain a log file no larger than the specified size. Deselect this option for unlimited log file size.

Enter the desired log file size in the provided spin box.

Displays a list of file extensions which VShield will scan.

Click this to add another file extension.

Click this to delete the selected file extension.

Click this to restore VShields default file extensions.

Enter new file extension here.

Click this to specify VShield log file location.

Selecting this option instructs VShield to create a log entry indicating the VShield settings for the computing session.

Selecting this option instructs VShield to create a log entry summarizing its activity during the computing session.

Selecting this option instructs VShield to scan for viruses on floppy disks during system shutdown.

Selecting this option instructs VShield to include the Windows user name when creating log entries.

Enter the path to the desired move folder for which infected files are to be moved. This folder will automatically be excluded from VShield scans.

Click this to locate a folder.

Selecting this option instructs VShield to scan for viruses on floppy disks which are accessed.

Selecting this option allows the user to disable VShield protection.

Selecting this option instructs VShield to appear as an icon on the desktop.

Selecting this option instructs VShield to create a log entry when an infected file has been detected.

Selecting this option instructs VShield to create a log entry when an infected file was successfully cleaned.

Selecting this option instructs VShield to create a log entry when an infected file has been deleted. Enabling this option allow you to track which files need to be restored from original diskettes or backup.

Selecting this option instructs VShield to create a log entry when an infected file has been moved to a move folder.

Selecting this option instructs VShield to include a date and time stamp with each log entry.

Selecting this option instructs VShield to scan for viruses in files which are launched.

Selecting this option instructs VShield to scan for viruses in files which are opened for copying to the local system.

Selecting this option instructs VShield to scan for viruses in files which are created on the local system.

Selecting this option instructs VShield to scan for viruses in files which are renamed on the local system.

Selecting this option instructs VShield to provide the Clean option when infected files are detected. Clean gives the user and VShield an opportunity to clean the infected file. Additional options will be provided if cleaning is unsuccessful.

Selecting this option instructs VShield to provide the Delete option when infected files are detected. Delete gives the user and VShield the opportunity to delete the infected file.

Selecting this option instructs VShield to provide the Exclude option when infected files are detected. Exclude removes this file from further scans for the computing session. Permanent exclusion can be found on the **Exclusions** property page.

Selecting this option instructs VShield to provide the Stop option when infected files are detected. Stop will discontinue with the access of the file.

Selecting this option instructs VShield to provide the Continue option when viruses are detected. Continue will bypass VShield warnings and allow the user to continue with the access of the file.

Objects, such as files, folders, or drives, defined in this list will be excluded from virus detection. Confirm that additions made to this list are free from infection.

Click this to add an object for exclusion from VShield scanning.

Click this to remove the highlighted entry from the Exclusions list.

Click this to edit the highlighted entry.

Click this to automatically load VShield during system startup.