Microsoft Anti-Virus Help

Commands	Reference to menu commands.
Procedures	Step-by-step instructions.
Keyboard Guide	Table of useful key combinations.
Glossary	Definitions of terms.

Commands

Scan Menu

- Detect
- Clean
- Delete CHKLIST files
- Virus List
- Exit Anti-Virus

Option Menu

- Set Options
- Save Settings on Exit

Related Topics

- Procedures

Procedures

- Removing Viruses
- Viewing the Virus List
- Defending Against Unknown Viruses

_____

Related Topics

Commands

Microsoft Anti-Virus Keys

Keys(s)	Function
Tab	Moves to the next command button, list box, text box, check box, or group of option buttons.
Shift+Tab	Moves to the previous list box, text box, check box, command button, or group of option buttons.
Arrow keys	Moves within an active group of options or command buttons.
Spacebar	Chooses the active command button or turns active check box on or off.
F1	Help
F10	Activates the menu bar.
Alt+F4	Closes the Anti-Virus program.
Enter	Chooses the active command button.
Esc	Cancels a command and closes the dialog box.

Related Topics

Commands

Detect (Scan menu)

Detect displays the Virus Found warning if it finds a file with a known virus. (Detect, unlike Clean, does not automatically remove the virus.) By default, Detect also warns you about executable files that have changed with the Verify Error warning.

Related Topics

Defending Against Unknown Viruses

Clean (Scan menu)

Choose Clean to remove known viruses automatically from your system. If the Verify Integrity option is on, Anti-Virus displays a Verify Error if it finds a changed executable file. (Since executable files generally don't change, modification could indicate infection by an unknown virus.)

_____

Related Topics

Detecting Viruses

Delete CHKLIST files (Scan menu)

Checklist files (CHKLIST.MS) store each executable file's size, MS-DOS attributes, date, and checksum. Anti-Virus and VSafe use these statistics to defend against unknown viruses.

To save disk space, you can delete the checklist files by selecting a drive and choosing Delete CHKLIST files. The verify integrity feature, however, will no longer work.

Related Topics

- Creating Checksums on Floppies
- Defending Against Unknown Viruses

Virus List (Scan menu)

This command displays a list of all the viruses recognized by Anti-Virus. The list shows each virus name, alias (if any), type, size, and the number of variants. To get detailed information on specific viruses, double-click the virus name or select the virus name and choose Info.

_____

Related Topics

Cleaning Viruses
Defending Against Unknown Viruses

Exit Anti-Virus (Scan menu)

This command exits Microsoft Anti-Virus. If you have selected the Save Settings On Exit option, any changes you have made to the program's configuration are saved.

_____

Related Topics

Setting Options

Set Options (Options menu)

Set Options allows you to configure Anti-Virus's options:

Verify Integrity
Create New Checksums
Create Checksums on Floppies
Disable Alarm Sound
Create Backup
Prompt While Detect
Anti-Stealth
Check All Files
Wipe Deleted Files

These settings are stored in the MWAV.INI file.

_____

Related Topics

Exiting Anti-Virus

Save Settings on Exit (Options menu)

This option saves your settings to the MWAV.INI file when you quit.

The MWAV.INI file is saved in the directory that contains the MWAV.EXE file unless you have specified an MSDOSDATA variable in your AUTOEXEC.BAT file. For example, if your AUTOEXEC.BAT file includes the following command, the MWAV.INI file is saved in the USER directory on drive C:

```
SET MSDOSDATA=C:\USER
```

Related Topics

Defending Against Unknown Viruses

Removing Known Viruses

To remove known viruses from your system:

1. Select the drive(s) you want to scan in the Drives list.
2. Choose Options if you need to change any Anti-Virus options.
3. Choose the **Clean** button.

Anti-Virus checks your system's memory for any viruses, scans the selected drive(s), removes any known viruses, and displays a summary report. If the verify integrity feature is on, then Anti-Virus displays a warning dialog box each time it discovers an executable file that has changed.

Related Topics

Wipe Deleted Files option

Viewing the Virus List

To examine a list of all the viruses recognized by Anti-Virus, choose Virus List from the Scan menu. Anti-Virus lists each virus by its most common name, with known aliases indented under the name. The list displays the virus type (Trojan, Boot, or file infector) along with the size of the virus code and the number of known strains, or variants, of the virus.

To find information about a virus, scroll through the list or type the first few characters of its name.

For detailed information on specific viruses, double-click the virus in the list or select it and choose Info.

Related Topics

Cleaning Viruses

Defending Against Unknown Viruses

Anti-Virus and VSafe contain virus databases that allow them to identify hundreds of specific viruses. To protect against new viruses that are not in the database, Microsoft Anti-Virus provides a verify integrity feature that looks for changes in executable files.

To make use of this protection, check to see that the Create New Checksums, Prompt While Detect, and Verify Integrity options are on. If they are, Anti-Virus alerts you about changed executable files during Detect scans. If VSafe is loaded, it alerts you whenever you attempt to run a changed file.

Related Topics

Creating Checksums on Floppies

Verify Integrity

This option enables Anti-Virus and VSafe to alert you to changes in executable files, based on statistics stored in checklist files. Changes in executable files can indicate the presence of a virus.

When Verify Integrity is on and you perform a Detect scan, Anti-Virus displays a Verify Error warning each time it finds an executable file that has changed.

When Verify Integrity is on, VSafe displays a warning when you try to run an executable file that has changed.

_____

Related Topics

Defending Against Unknown Viruses

Create New Checksums

Use this option to take advantage of the verify integrity feature, your best defense against unknown viruses. If Create New Checksums is on, Anti-Virus creates a checklist file (CHKLIST.MS) for each directory it scans. This file contains statistics about each executable file in the directory, including the file's size, date, and MS-DOS attributes. On subsequent scans, Anti-Virus can use these statistics to verify that the files have not changed. (If a file has changed, it may be infected by a virus, since executable files normally do not change.)

VSafe's file verification check also uses the checklist file to defend against unknown viruses.

Related Topics

- Creating Checksums on Floppies
- Deleting CHKLIST files
- Defending Against Unknown Viruses
- Verify Integrity option

Create Checksums on Floppies

Use this option to take advantage of the verify integrity feature, your best defense against unknown viruses. If Create New Checksums on Floppies and Create New Checksums are enabled, Anti-Virus creates a checklist file (CHKLIST.MS) for each directory it scans on the floppy. This file contains statistics about each executable file in the directory, including the file's size, date, and MS-DOS attributes. On subsequent scans, Anti-Virus can use these statistics to verify that the files have not changed. (If a file has changed, it may be infected by a virus, since executable files normally do not change.)

VSafe's file verification check also depends on the checklist file.

Related Topics

- Deleting CHKLIST files
- Defending Against Unknown Viruses

Disable Alarm Sound

Select this option if you do not want to hear a sound played when a warning message appears or when a virus is located or cleaned. The sound is useful for getting your attention, but not required when you're using Anti-Virus.

This option does not affect VSafe.

_____

Related Topics

Commands

Create Backup

When this option is on, Anti-Virus makes a backup of any file infected with a virus before cleaning the original file. The backup file is renamed with a VIR extension.

Using this option can be dangerous, however, because it means a virus-infected file remains on your disk. You should only use this option if, for example, the infected file is your only copy of a program and you would rather use an infected program than not have it at all.

_____

Related Topics

Commands

Prompt While Detect

When this option is on, Anti-Virus displays the Verify Error and Virus Found warnings during Detect scans. If Prompt While Detect is off, Anti-Virus does not provide any warnings during the Detect scan.

Related Topics

Setting Options

Anti-Stealth

Anti-Virus's verify integrity feature protects your system against unknown viruses. Unknown Stealth viruses, however, can evade this protection by using a special technique which allows them to infect files without appearing to change them.

To detect unknown Stealth viruses, choose the Anti-Stealth option and make sure the Verify Integrity option is also selected. Anti-Virus will then use a low-level verification technique during Detect scans that will find and alert you to Stealth-infected files.

This option does not affect VSafe.

_____

Related Topics

Setting Options

Check All Files

When this option is selected, all files are checked for viruses. When turned off, only executable files are checked. Executable files end with the extensions EXE, COM, OV*, SYS, BIN, APP, CMD, PGM, PRG, DRV, DLL, 386, FON, APP, ICO, or PIF.

_____

Related Topics

Setting Options

Wipe Deleted Files

This option modifies the Virus Found warning that Anti-Virus displays when it detects a virus. Normally, this dialog box provides you with a Delete button. If the Wipe Deleted files option is on, however, this button changes to Wipe. If you select Wipe, Anti-Virus overwrites each cluster of the infected file so that every trace of it is eradicated.

_____

Related Topics

Detect command

Verify Error Warning

This dialog box alerts you that a system or executable file has changed, based on the information stored in checklist files. Since changes in system and executable files can indicate an unknown virus, the dialog box provides the following options:

Update: Choose this option if there is a valid reason for the change. Anti-Virus then updates checklist file with the executable file's new statistics to prevent future alert messages.

Delete or **Repair:** If Delete appears, it means the file's size or checksum has been altered. Choose this option if your system appears to be infected and you can't account for the change to the file. If Repair appears, only the file's date or time has been modified and it is not infected. Choose this option to restore the file's date and time to its original settings.

Stop: Choose this option to halt the scan.

Continue: Choose this option to continue the scan with no changes.

NOTE: This dialog box only appears if the Verify Integrity and Prompt While Detect options are on.

Virus Found Warning

If you are using the Detect feature and a known virus is found in one of your files, you have the following options:

Clean: Choose this option to remove the virus from the file.

Stop: Choose this option to halt the scan.

Delete or **Wipe**: The Delete option is the default. Choose Delete to perform a MS-DOS deletion of the file. The Wipe option appears if the Wipe Deleted Files setting is on. When you wipe a file, Anti-Virus overwrites all of its clusters and eradicates every trace of the infected file.

Continue: Choose this option to continue the scan with no changes.

Glossary

Boot sector virus

Checklist file

Checksum

Executable file

File infectors

Known virus

Trojan horse

Unknown virus

Verify integrity

Virus

VSafe

Boot Sector Virus

A virus that copies itself to the boot sector of a computer's hard or floppy disk. Boot sector viruses replace the disk's original boot sector with their own code so that the virus is always loaded into memory before anything else. Once in memory, the virus can spread to other disks.

Checklist File

The checklist file (CHKLIST.MS) stores the checksum, MS-DOS attributes, size, and the date and time of executable and system files. If the Verify Integrity option is on, Anti-Virus and VSafe use the checklist file to watch for changes in executable files.

Checksum

A numerical value derived from the individual bytes of the file. Along with the file's date, size, and MS-DOS attributes, the checksum is stored in checklist files (CHKLIST.MS) created by Anti-Virus.

Executable File

For the purposes of virus detection, any file with the following extensions: EXE, COM, OV*, SYS, BIN, APP, CMD, PGM, PRG, DRV, DLL, 386, FON, APP, ICO, and PIF.

File Infectors

File infectors add their virus code to executable files. Once the virus is executed, it spreads to other executable files.

Known Virus

Anti-Virus and VSafe contain virus databases that allow them to recognize hundreds of specific viruses. A "known virus" is a virus that appears in this database. To see a list of the known viruses, select Virus List from the Scan menu.

Trojan Horse

A type of virus that is disguised as a legitimate program. Trojan horses are much more apt to destroy files or damage disks than other viruses.

Unknown Virus

Anti-Virus and VSafe each contain virus databases that allow them to recognize hundreds of specific viruses. An "unknown virus" is a virus that does not appear in this database. To see a list of the known viruses, select Virus List from the Scan menu.

Verify Integrity Feature

You can configure Anti-Virus and VSafe to watch for changes in executable files and issue a Verify Error if they discover any. Since system and executable files normally don't change, a Verify Error may indicate that there is an infection.

Virus

A program designed to replicate and spread on its own. Microsoft Anti-Virus recognizes hundreds of specific viruses and can also protect your system against unknown virus strains using its Verify Integrity feature.

VSafe

VSafe is a memory-resident utility that monitors your system for known viruses whenever a program is executed. Additionally, VSafe monitors your system for suspicious activities that may indicate viruses.