



Norton AntiVirus Network Manager Help Contents

▼ Expand

Overview

Procedures

Commands

Dialog Boxes

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

▼ Expand

Overview

- [!\[\]\(cf5be311f7b2821912d8009884508fa2_img.jpg\) What Network Manager Does](#)
- [!\[\]\(9804e70d96ff9fe9899b264c06a33cd7_img.jpg\) How Network Manager Works](#)
- [!\[\]\(4f49380f3d6bce047bc47b2072cc076f_img.jpg\) Educating Your Users](#)
- [!\[\]\(73944fd4f6fb83e4c64013731d1820cc_img.jpg\) Using Intelligent Updater](#)
- [!\[\]\(d8f7165d5a8d1eba426ea452457190e5_img.jpg\) Staying Protected](#)
- [!\[\]\(f608c4821f4fa8f3141b1baf96fa88f9_img.jpg\) Troubleshooting](#)

Procedures

Commands

Dialog Boxes

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

Expand

Overview

Procedures

- [!\[\]\(511a36c244659513b679df9c639945de_img.jpg\) Creating Setup Files for Workstations](#)
- [!\[\]\(2c0783baf87a2728b2fe49eb1c34c456_img.jpg\) Customizing Installation](#)
- [!\[\]\(7cfb20e3a97beaa6243bf39ce8dc849f_img.jpg\) Setting Pre- and Post-Install Actions](#)
- [!\[\]\(4ec82d7d2c97e7458ec11741fc48dcdc_img.jpg\) Customizing User Registration](#)
- [!\[\]\(8a3eeabae8fd8c34f983be60adf65fec_img.jpg\) Setting Additional Windows Options](#)
- [!\[\]\(f8c4514865ca6cc7d15601f5b468a267_img.jpg\) Saving Your Changes to a Setup File](#)
- [!\[\]\(3e3a16082679d4e25573352df409eccd_img.jpg\) Updating a User's Login Procedure](#)
- [!\[\]\(9b1df3f6f95a7aa10cbc22e7842da063_img.jpg\) Customizing Scanner Options](#)
- [!\[\]\(7936f9bcfbfb218ad8be8ab6d2aa8317_img.jpg\) Customizing Automatic Protection](#)
- [!\[\]\(7b335444bdd8e9de4c89d81708f76337_img.jpg\) Customizing Alerts](#)
- [!\[\]\(65abe31c0ef71e56cf853e9b6273e467_img.jpg\) Customizing Inoculation](#)
- [!\[\]\(7a2fa42399a378955de1effe4cf6b043_img.jpg\) Customizing the Activity Log](#)
- [!\[\]\(08c0a656573a88d33d475c29e72a29c0_img.jpg\) Customizing Password Protection](#)
- [!\[\]\(5bdd610281e86439b007b8e48679cd03_img.jpg\) Modifying the Exclusions List](#)
- [!\[\]\(2c5385ce0863a8e79f0c4c163148e63b_img.jpg\) Viewing the Exclusions List](#)

Commands

Dialog Boxes

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

▼ Expand

Overview

Procedures

Commands

File Menu

Tools Menu

Help Menu

Dialog Boxes

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents






▼ Expand

Overview

Procedures

Commands

File Menu

-  New Setup
-  Open Setup
-  Save Setup
-  Save Setup As
-  Exit

Tools Menu

Help Menu

Dialog Boxes

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

▼ Expand

📁 Overview

📁 Procedures

📁 Commands

📁 File Menu

📁 Tools Menu

▢ Options

📁 Help Menu

📁 Dialog Boxes

📁 Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

▼ Expand

Overview

Procedures


Commands


File Menu

Tools Menu

Help Menu

 Contents

 Procedures

 Commands

 How to Use Help

 About...

Dialog Boxes

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

▼ Expand

Overview

Procedures

Commands

Dialog Boxes

- [Open Setup File](#)
- [Save Setup File As](#)
- [Categories of Options - Settings](#)
- [Install/Update Settings Reference](#)
- [Before and After Installing/Updating](#)
- [User Registration](#)
- [Windows](#)
- [Scanner Settings Reference](#)
- [Scanner Advanced Settings](#)
- [Auto-Protect Settings Reference](#)
- [Auto-Protect Advanced Settings](#)
- [Auto-Protect Startup Settings](#)
- [Auto-Protect Virus Sensor Settings](#)
- [Alerts Settings Reference](#)
- [Alert Others Settings Reference](#)
- [Activity Log Settings Reference](#)
- [Exclusions List Settings Reference](#)
- [Add/Edit Exclusion](#)
- [Inoculation Settings Reference](#)
- [Password Settings Reference](#)
- [Set/Change Password](#)
- [General Settings Reference](#)

Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents

▼ Expand

📁 Overview

📁 Procedures

📁 Commands

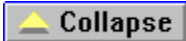
📁 Dialog Boxes

📁 Keyboard Shortcuts

▢ Keyboard Shortcuts



Norton AntiVirus Network Manager Help Contents



Overview

[What Network Manager Does](#)

[How Network Manager Works](#)

[Educating Your Users](#)

[Using Intelligent Updater](#)

[Staying Protected](#)

[Troubleshooting](#)

Procedures

[Creating Setup Files for Workstations](#)

[Customizing Installation](#)

[Setting Pre- and Post-Install Actions](#)

[Customizing User Registration](#)

[Setting Additional Windows Options](#)

[Saving Your Changes to a Setup Files](#)

[Updating a User's Login Procedure](#)

[Customizing Scanner Options](#)

[Customizing Automatic Protection](#)

[Customizing Alerts](#)

[Customizing Inoculation](#)

[Customizing the Activity Log](#)

[Customizing Password Protection](#)

[Modifying the Exclusions List](#)

[Viewing the Exclusions List](#)

Commands

File Menu

[New Setup](#)

[Open Setup](#)

[Save Setup](#)

[Save Setup As](#)

[Exit](#)

Tools Menu

[Options](#)

Help Menu

[Contents](#)

[Procedures](#)

[Commands](#)

[How to Use Help](#)

[About...](#)

Dialog Boxes

[Open Setup File](#)

[Save Setup File As](#)

[Options Dialog Box](#)

[Install/Update Settings](#)

[Before and After Installing/Updating](#)

[User Registration](#)

[Windows](#)

[Scanner Settings Reference](#)

[Scanner Advanced Settings](#)

[Auto-Protect Settings Reference](#)

[Auto-Protect Advanced Settings](#)

[Auto-Protect Startup Settings](#)

[Auto-Protect Virus Sensor Settings](#)

[Alerts Settings Reference](#)

[Alert Others](#)

[Activity Log Settings Reference](#)

[Exclusions Settings Reference](#)

[Add Exclusions](#)

[Inoculation Settings Reference](#)

[Password Settings Reference](#)

[Set Password](#)

[General Settings Reference](#)

Keyboard Shortcuts

[Keyboard Shortcuts](#)

Credits

[Credits](#)



Keyboard Shortcuts

Keyboard Shortcuts



Commands

File Menu

[New Setup](#)

[Open Setup](#)

[Save Setup](#)

[Save Setup As](#)

[Exit](#)

Tools Menu

[Options](#)

Help Menu

[Contents](#)

[Procedures](#)

[Commands](#)

[How to Use Help](#)

[About...](#)



Procedures

[Creating Setup Files for Workstations](#)

[Customizing Installation](#)

[Setting Pre- and Post-Install Actions](#)

[Customizing User Registration](#)

[Setting Additional Windows Options](#)

[Saving Your Changes to a Setup File](#)

[Updating a User's Login Procedure](#)

[Customizing Scanner Options](#)

[Customizing Automatic Protection](#)

[Customizing Alerts](#)

[Customizing Inoculation](#)

[Customizing the Activity Log](#)

[Customizing Password Protection](#)

[Modifying the Exclusions List](#)

[Viewing the Exclusions List](#)



Overview

What Network Manager Does

How Network Manager Works

Educating Your Users

Using Intelligent Updater

Staying Protected

Troubleshooting



Install/Update Settings Reference

Use these settings to customize how NAVUPDTW.EXE installs the Norton AntiVirus program on users' systems.

Network Directory to Install From: Type the network path that contains the Norton AntiVirus files, or select the browse button to see a list of paths from which you can choose the network path. Use the server name and path, not drive letters. For example, on a Novell network, a valid pathname is \\SERVER1\SYS:PUBLIC\NAV.

NOTE: You do not normally have to select anything because your current directory is the default. You do not have to specify the current directory.

Local Directory to Install To: Specifies where you want Norton AntiVirus installed on the workstation.

Use Previous Directory: Overwrites an existing version of Norton AntiVirus if found on the workstation. (This option assumes the Norton AntiVirus directory is in the workstation's PATH statement.)

If a previous version of Norton AntiVirus is not found, the user is either prompted for a location or Norton AntiVirus is installed into the directory specified in the Use Default text box (depending on which other option is selected).

Prompt: Lets the user decide where to install Norton AntiVirus.

Use Default: Installs Norton AntiVirus to the drive and directory you specify in the text box.

Modify AUTOEXEC.BAT: Specifies what to add to the workstation's AUTOEXEC.BAT file.

Run NAV.EXE: Causes Norton AntiVirus to scan the user's workstation each time it starts up.

Add NAV Directory to Path: Adds the pathname where Norton AntiVirus resides to the workstation's search path.

Auto-Protect: Specifies how you want the automatic protection feature set up on the workstation.

Install in CONFIG.SYS: Causes the automatic protection feature command line to be added to the workstation's CONFIG.SYS file.

Do not Install: Does not add the automatic protection feature to the workstation's startup files.

Install in AUTOEXEC.BAT: Causes the automatic protection feature command line to be added to the workstation's AUTOEXEC.BAT file.

Retain Settings When Updating: Check this option to prevent updating of the user's configuration settings when installing or updating the Norton AntiVirus executable files or the virus definitions files.

NOTE: This does not apply when updating from versions previous to NAV 3.0.

Force Logoff If Auto-Protect Not Installed: Check this option to prevent users from logging onto the network when the automatic protection feature is not enabled on their workstations.

Confirm All Prompts: Allows the user to verify information entered for user registration and directory to install to.

Buttons:

Before...: Allows you to set Norton AntiVirus activity before installing or upgrading. See [Before and After Installing/Updating](#)

User...: Allows you to require user registration. See [User Registration](#)

Windows...: Allows you to specify which portions of Norton AntiVirus for Windows is

installed on the workstation. See [Windows](#).



Before and After Installing/Updating

Use these settings to specify what to do before and after installing Norton AntiVirus on a workstation.

Before Installing/Updating

Scan Memory: Scans the workstation's RAM for viruses.

Scan Hard Disk System Areas: Scans the workstation's hard disk boot records for viruses.

Scan Program Files: Scans all program files on the workstation's hard disk.

Scan Always: Scans the above selections every time the workstation logs on to the network.

Command to Execute Before Install/Update: Causes a specified program to run before Norton AntiVirus is installed. Type the command (up to 128 characters) in the text box or select the browse button to choose a command.

Execute Command Always: Causes the program specified in the **Command to Execute...** text box to run every time the workstation logs on to the network.

After Installing/Updating

Action:

Prompt to Reboot: Gives the user the option to reboot or not.

Do not Reboot: Does not restart the workstation after Norton AntiVirus is installed or updated. Automatic Protection will not be enabled or updated until the next time the user restarts the system.

Reboot: Restarts the workstation automatically after Norton AntiVirus is installed.

Command to Execute After Install/Update: Causes a specified program to run after Norton AntiVirus is installed. Type the command (up to 128 characters) in the text box or select the browse button to choose a command.

Execute Command Always: Causes the program specified in the Command to Execute... text box to run every time the workstation logs on to the network, regardless of whether Norton AntiVirus is being installed or updated.



User Registration

Use these settings to customize user registration. To save the settings, select OK.

Prompt: Prompts to let the user enter the company name. If you enter text in the Use Default text box, it is offered to the user as a default selection.

Use Default: Uses the company name you enter in the text box.

Prompt for Name: Prompts the user to enter his or her name.



Windows

Use these settings to install Norton AntiVirus for Windows on workstations. To save the settings, select OK.

Install NAV for Windows: Installs Norton AntiVirus for Windows on workstations.

Load Windows Drivers: Installs automatic protection for Windows.

Create Windows Group: Creates a new Windows group called "Norton AntiVirus" on the workstation.



Customizing Scanner Options

The settings for the Scanner category of options define what Norton AntiVirus does when you scan a file, directory, or drive, using the commands in the Scan menu or using the Scan Now command button.

To customize scanning:

- 1 Choose **Options...** from the Tools menu. Select the Scanner category at the left side of the Options dialog box.
The Options - Scanner Settings dialog box appears.

- 2 Specify in the **What To Scan** group box the areas Norton AntiVirus scans before it scans files:

Memory: Checks for viruses resident in your computers memory, so they will not spread to all of the files you scan.

Master Boot Record: Checks for boot viruses in the master boot record on your hard disk.

Boot Records: Checks for boot viruses in the boot records on your hard disk and on any floppy disks that you scan.

We recommend that you check all of these options.

- 3 Specify what files you want to scan:

All Files: Scan all files in the specified directory or drive. This includes files less likely to contain viruses.

Program Files Only: Scans files that are most likely to become infected. Only the files with an extension that is specified in the program file extensions list are scanned.

- 4 Check **Within Compressed Files** to have Norton AntiVirus scan files compressed using the PKZIP utility.

Scanning time may increase slightly if you have many .ZIP files. If you have no .ZIP files, scanning time is not affected by having this option selected.

- 5 Select an option in the **When a Virus is Found** drop-down list box:

Prompt: Informs you when a virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.

Notify Only: Merely informs you when a virus is detected. You will not be able to repair or delete the infected file.

Repair Automatically: Repairs an infected file or boot record without notifying you. The results of the repair will be displayed at the end of the scan. Note that Norton AntiVirus is preset to make backup copies of files before they are repaired.

Delete Automatically: Deletes an infected file without notifying you. The file deletion will be displayed at the end of the scan. Use caution when selecting this option. Files deleted by Norton AntiVirus cannot be recovered.

Halt Computer: Halts your computer when a virus is detected. You must then restart your computer.

- 6 If you selected Prompt in Step 5, choose from the following **Buttons to Display if Prompted** group box which options you want Norton AntiVirus to make available when a virus is found:

Repair: Allows you to repair the file. If the virus infects an item that cannot be repaired, such as a compressed file, the button will be dimmed.

Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button will be dimmed.

Continue: Allows you to continue scanning without resolving the problem. The Continue button applies only when Immediate Notification is turned on. See step 8 for details about Immediate Notification.

Exclude: Allows you to exclude this file from future checks for known viruses. Use caution when enabling this button; it can reduce your protection against viruses.

- 7** Select Advanced....
The Scanner Advanced Settings dialog box appears.
- 8** Check the options you want to enable:
 - Allow Network Scanning:** Allows you to scan entire network drives. Scanning network drives is more time-consuming than scanning local drives.
 - Allow Scanning to be Stopped:** Allows you to halt a scan in progress. When this option is checked, the Stop button is available during a scan.
 - Immediate Notification:** Displays an alert box when a problem is detected while scanning. This allows you to respond immediately, instead of waiting until the scan is completed.
- 9** Specify in the **Preselect at Start** group box the drives that you want selected automatically in the Drives list box when you start Norton AntiVirus.
- 10** Select OK in the Scanner Advanced Settings dialog box.
- 11** Select OK in the Options - Scanner Settings dialog box.



Customizing the Activity Log

You can specify the name and location for the activity log file, the types of events to record, and a maximum size for the file.

To customize the activity log:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Activity Log category on the left side of the Options dialog box. The Options - Activity Log Settings dialog box appears.
- 3 In the **Log Following Events** group box, check each type of event that you want Norton AntiVirus to record:
 - Known Virus Detections:** Records detections of known viruses.
 - Unknown Virus Detections:** Records detections of unknown viruses.
 - Inoculation Activities:** Records detections of uninoculated files and changes in a file's inoculation data.
 - Virus-Like Activities:** Records detections of virus-like activities, such as an attempt to format your hard disk.
 - Completion of Scans:** Records the date and ending time of scans that you initiate.
 - Virus List Changes:** Records changes to the virus list.
- 4 If you want to limit the size of the activity log file, check **Limit Size of Log File To**, then enter the desired size in the **Kilobytes** text box. When the specified file size is reached, each new entry added to the activity log will cause the oldest entry or entries to be deleted.
- 5 Enter the pathname for the activity log file in the **Activity Log Filename** text box.
Or,
Use the browse button to select an existing file or a path for a new file.
- 6 Select OK.



Customizing Automatic Protection

The automatic protection feature of Norton AntiVirus is a terminate-and-stay-resident program (TSR) and is loaded when you start up your computer, so you are protected from viruses as soon as you start working.



Customizing Alerts

You can customize how Norton AntiVirus informs you that it has detected a virus or suspicious virus-like activity:

To customize alerts:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the **Alerts** category on the left side of the Options dialog box. The Options - Alerts Settings dialog box appears.
- 3 Check any or all of the following categories:
 - Display Alert Message:** Lets you add a message with instructions or special warnings to all alerts that Norton AntiVirus displays. You can then enter a message of up to 76 characters in the text box.
 - Audible Alert:** Sounds a tone when Norton AntiVirus alerts you of a virus.
 - Remove Alert Dialog After:** Removes notification dialog boxes after a specified number of seconds. You can enter a number between 1 and 99 in the **Seconds** text box.
- 4 Use the **Alert Others** group box to specify where you want Norton AntiVirus to send alerts over the network.
 - Alert Network Users:** Messages from Norton AntiVirus are sent to other users on your network. Type the names of the users in the text box or select the browse button and select the users from the list that appears.
 - Alert Network Console:** Messages from Norton AntiVirus are sent to the network server.
 - Alert Norton AntiVirus NLM If Present:** Messages from Norton AntiVirus are sent to the Norton AntiVirus NetWare Loadable Module (NLM) if it is present on your network.
- 5 If you checked an option in step 4, select **Others...** The Alert Others dialog box appears.
- 6 Select the types of alerts you want to broadcast over your network, then select OK.
- 7 Select OK in the Options - Alerts Settings dialog box.



Customizing Inoculation

The first step to inoculating files and boot records during a scan is to customize the inoculation options.

To customize inoculation options:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Inoculation category on the left side of the Options dialog box. The Options - Inoculation Settings dialog box appears.
- 3 Check **Inoculate Boot Records and System Files** to check the master boot record, boot records, and system files on your hard disk for inoculation.
We recommend you check this option, since it is the only means by which Norton AntiVirus can detect unknown viruses in boot records.
- 4 Check **Inoculate Program Files** to check files for inoculation on the hard disks and network drives you use. Then check **Inoculate Files On Floppies** if you also want to use inoculation for files on the floppy disks you use.
- 5 Select an option in the **When An Item Has Not Been Inoculated** drop-down list box:
 - Prompt:** Informs you when a program file or boot record has not been inoculated and lets you choose how to respond.
 - Inoculate Automatically:** Inoculates each uninoculated program file or boot record as soon as it is detected.
 - Notify Only - Do not Inoculate:** Norton AntiVirus merely informs you that a program file or boot record is not inoculated. It will not inoculate the item.
 - Deny Access:** Informs you that a program file has not been inoculated and does not allow you to use the program. This options does not apply to uninoculated boot records.
- 6 Select an option in the **When An Inoculated File Has Changed** drop-down list box. See descriptions of your choices in step 5:
 - Prompt**
 - Notify Only - Do not Reinoculate**
 - Deny Access**
- 7 If you selected Prompt after either step 5 or 6 or both, specify in the **Buttons to Display If Prompted** group box which options you want Norton AntiVirus to make available when an inoculation issue is found.
 - Repair:** Allows you to repair a program file or boot record with an inoculation change, returning the item to its state when it was last inoculated.
 - Delete:** Allows you to delete a program file with an inoculation change. Boot records cannot be deleted.
 - Inoculate:** Allows you to inoculate a program file or boot record or reinoculate a changed program file or boot record.
 - Continue:** Allows you to continue the current operation (scanning or accessing a program file). No change is made to the inoculation data.
 - Stop:** Allows you to stop the current operation (scanning or accessing a program file). No change is made to the inoculation data.
 - Exclude:** Allows you to exclude the program file from future checks for inoculation changes.
- 8 Type a pathname for the inoculation files in the **Inoculation Path** text box. When you inoculate program files and boot records, an inoculation file is placed in the specified location on each drive you inoculate. If you are inoculating files on network drives, you must have read-write access privileges to this directory on the network

drive. You do not need read-write access to the files you inoculate.

- 9 Select OK.



Customizing Password Protection

You can add password protection to selected features of Norton AntiVirus to prevent unauthorized access.

To password protect features:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Password category on the left side of the Options dialog box. The Options - Password Settings dialog box appears.
- 3 Check **Password Protect** to turn on the password protection feature.
- 4 If you want to protect all of the features shown in the list box, select **Maximum Password Protection**.

Or,

If you would like to protect only certain features, select **Custom Password Protection**; then select the features you would like to protect in the list box.

- 5 Select **Set Password...** to set a password. The Set Password dialog box appears.
- 6 Type a password in the **New Password** text box, then type it again in the **Confirm New Password** text box.

Passwords can be from 1 to 16 characters in length and are not case-sensitive ("a" is the same as "A"). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (*) for security.

TIP: Write down your password and store it in a secure place.

- 7 Select OK in the Set Password dialog box.
- 8 Select OK in the Options - Password Settings dialog box.

Password protection will activate the next time you start Norton AntiVirus. The password must be entered the first time you use a protected feature.

NOTE: Norton AntiVirus will also prompt for the password before allowing changes to the password protection options.

See also:

[Password Settings Reference](#)



New Setup

Use this command to create a new setup file that specifies configuration settings for installing Norton AntiVirus on users' workstations.



Open Setup

Use this command to open an existing setup file.



Save Setup

Use this command to save a setup file.



Save Setup As

Use this command to save a setup file with a different name.



Exit

Use this command to exit Norton AntiVirus Network Manager.



Categories of Options - Settings

Select a category name to see help for that category's settings.

Install/Update

Scanner

Auto-Protect

Alerts

Activity Log

Exclusions List

Inoculation

Password

General



Activity Log Settings Reference

Use these settings to determine what events Norton AntiVirus records in the activity log.

Log Following Events:

Known Virus Detections: Records known virus detections.

Unknown Virus Detections: Records unknown virus detections.

Inoculation Activities: Records detections of uninoculated files and files that have changed since they were inoculated.

Virus-Like Activities: Records virus-like activity detections.

Completion of Scans: Records end times of scans that you initiate.

Virus List Changes: Records deletions and updates that you make to the virus list.

Limit Size of Log File to (amount) Kilobytes: Sets size of activity log file. When the file grows to the size you specify, Norton AntiVirus starts deleting the oldest entries as it adds new ones.

Activity Log Filename: Lets you type a path and filename for the activity log file. You can also select the browse button to go to the Log File dialog box to select an existing file or a path for a new file.



Alerts Settings Reference

Use these settings to configure the way Norton AntiVirus informs you and others of events. For directions, see [Customizing Alerts](#).

Display Alert Message: Tells Norton AntiVirus to add your text to its alert messages. You can enter up to 76 characters in the text box.

Audible Alert: Tells Norton AntiVirus to sound a tone when it detects a virus.

Remove Alert Dialog After (X) Seconds: Specifies the number of seconds (between 1 and 99) that a notification dialog stays on your screen.

Alert Others

Use these settings to set network-specific options.

Alert Network Users: Messages from Norton AntiVirus are sent to other users on your network. Type the names of the users in the text box or select the browse button and select users from the list that appears.

Network Console: Messages from Norton AntiVirus are sent to the network server.

Alert Norton AntiVirus NLM If Present: Messages from Norton AntiVirus are sent to the Norton AntiVirus NetWare Loadable Module (NLM) if it is present on your network.

Others... Button: If you checked an option in the Alert Others group box, select this button. It opens the [Alert Others](#) dialog box, where you select the types of events to inform other network users about.



Alert Others

Use these settings to determine what alerts to send to the network users you selected. For directions, see [Customizing Alerts](#).

Alert Others When

Known Virus Detections: Norton AntiVirus detects a virus that it can identify by name.

Unknown Virus Detections: Norton AntiVirus detects a virus for which it has no virus definition.

Inoculation Activities: Norton AntiVirus detects an uninoculated file or a change in a file's inoculation data.

Virus-Like Activities: Norton AntiVirus detects an activity that it perceives as the work of a possible unknown virus.

Completion of Scans: Informs others when a scan ends.

Virus List Changes: Informs others when any modifications are made to the virus list.

See also:

[Alerts Settings Reference](#)



Exclusions List Settings Reference

An exclusion is a condition or activity that would normally be detected during a scan, but you have told Norton AntiVirus not to look for in a particular file.

Use the Exclusions List settings to view and change files you want excluded from selected Norton AntiVirus protection. You use the Add..., Edit..., and Delete buttons to make changes to the list.

Select a file in the **Items** group box to see what activities it is excluded from.

Add...: Define exclusions for a file, group of files using wildcards, or a directory.

Edit: Change the exclusions for a selected file.

Delete: Remove a selected file and its exclusions from the exclusions list.

NOTE 1: Excluding files reduces your protection level. Use sparingly. Also be advised that renaming or moving a file invalidates its exclusions.



Add/Edit Exclusion

Item...

Type the pathname for the file, group of files using wildcards, or a directory in the text box or use the browse button to select a single file from a list.

Include Subdirectories: Also exclude files in the subdirectories of the item. Only applies if the item is a directory.

Exclude From...

Known Virus Detection: Exclude the item from checks for known viruses.

Unknown Virus Detection: Exclude the item from checks for unknown viruses.

Inoculation Detection: Exclude the item from checks to see if it has been inoculated and for inoculation changes.

Low-Level Format of Hard Disk: Exclude the item from checks for attempts to perform a low-level format of your hard disk, which obliterates all information on the disk.

Write to Hard Disk Boot Records: Exclude the item from checks for attempts to write to the boot records on your hard disk. This is only performed legitimately by very few programs.

Write to Floppy Disk Boot Records: Exclude the item from checks for attempts to write to the boot record on a floppy disk. This action is performed legitimately by few programs.

Write to Program Files: Exclude the item from checks for attempts to write to a program file. Some programs save configuration information within themselves rather than in a separate file.

Read-Only Attribute Change: Exclude the item from checks for attempts to change a read-only file so that it can be written to.



Select Exclude File

Select a drive and directory. Choose a single filename from the list.



General Settings Reference

Use these settings to configure general Norton AntiVirus activity.

Backup File When Repairing: Norton AntiVirus makes a copy of the infected file before repairing it.

Enter an extension to be used for the backup file (the default is .VIR). If you have more than one backup for the same file, the extension will be modified successively (that is, .VIR, .VI1, .VI2, and so on). You should delete all backup files when you know that the repair operation was successful. Be advised that all files with the backup extension will be added to the exclusions list and will not be checked for known viruses.

LiveUpdate Automation: Norton AntiVirus launches LiveUpdate automatically when virus definitions files need updating. It is recommended that you check this.

Open files - shared mode: This option is unchecked by default. When unchecked, the shared mode flag is not set when a file is opened for scanning. This may not allow optimum performance in all network situations. Selecting this option, which opens files in shared mode, may, in some cases, improve performance.

Exclusion test before scan: This option is unchecked by default. When unchecked, scanning proceeds and the Exclusions list is examined only if a virus is detected. Selecting this option causes the Exclusions list to be checked before scanning proceeds. In some cases performance is improved by leaving this option unchecked.

Show Performance options on workstation: Check to allow users to have access to the above two options on their workstations.

Enable/Disable menu items on buttons: Checked options are available from the Norton AntiVirus main window on each networked workstation. Uncheck any option to disable it.



Password Settings Reference

Use these settings to define what features you want password-protected and to set or change the password. For directions, see [Customizing Password Protection](#).

Password Protect: Activates the Set Password button so you can open the [Set Password dialog box](#) and set a password. Turning this off removes all password protection.

Maximum Password Protection: Sets password protection for all Norton AntiVirus features listed. You will not be able to access any of these features without the password.

Custom Password Protection: Sets password protection for the items you select in the list box. You will not be able to access any of these features without the password.

Customizing Password Protection
Set/Change Password



Set/Change Password

Before setting or changing your password, make sure you've selected the items you want protected. See [Customizing Password Protection](#) for instructions.

Passwords can be from 1 to 16 characters in length and are not case-sensitive ("a" is the same as "A").

Old Password: If this is the first time you've created a password, this text box is dimmed. If you are changing a password, type the old one here.

New Password: Type the new password in the text box. As you type, Norton AntiVirus replaces the characters in your password with asterisks (*) on the screen for security.

Confirm New Password: Type the new password again in this text box. The features you selected are password-protected the next time you start Norton AntiVirus.



Inoculation Settings Reference

Use these settings to change inoculation activity. You can inoculate the boot records and system files on your hard disk and any program file. Norton AntiVirus uses the [program file extensions](#) list to determine if a file is a program file. For directions, see [Customizing Inoculation](#). For more information, select the See Also button at the top of this window.

Inoculate Boot Records and System Files: Causes Norton AntiVirus to inoculate the master boot record, boot records, and system files on your hard disk during the next scan you perform. This information is checked on every scan.

Inoculate Program Files: Causes Norton AntiVirus to inoculate all program files on hard disks and network drives.

Inoculate Files on Floppies: Causes Norton AntiVirus to also inoculate all program files on floppy disks.

How to Respond...

When an Item has not been Inoculated:

Select one of these options from the drop-down list box:

Prompt: Informs you when it finds an uninoculated program file or boot record and allows you to choose how to respond.

Inoculate Automatically: Inoculates each uninoculated program file and boot record as soon as it is detected.

Notify Only - Do not Inoculate:

Informs you but takes no action when it encounters an uninoculated program file or boot record.

Deny Access : Informs you that a program file is not inoculated and prevents you from using that file. This option does not apply to boot records.

When an Inoculated Item has Changed:

Select one of these options from the drop-down list box:

Prompt: Informs you when it finds a program file or boot record that has changed and allows you to choose how to respond.

Notify Only - Do not Inoculate: Informs you but takes no action when it encounters a changed file or boot record.

Deny Access: Informs you that a program file has changed and prevents you from using that file. This option does not apply to boot records.

Buttons to Display if Prompted:

Select the buttons you want to appear when an inoculation issue is found:

Repair: Allows you to repair a file or boot record with an inoculation change.

Delete: Allows you to delete a file with an inoculation change. Boot records cannot be deleted.

Inoculate: Allows you to inoculate or reinoculate the file or boot record.

Continue: Allows you to continue scanning or accessing the file with no change to its inoculation data.

Stop: Allows you to stop scanning or accessing the file with no change to its inoculation data.

Exclude: Allows you to exclude the file from future inoculation checks.

Inoculation Path: Type a directory for the inoculation file.

When you inoculate program files and boot records, an inoculation file is placed in the specified location on each drive you inoculate.



Auto-Protect Settings Reference

Use these settings to automate protection. For directions, see [Customizing Automatic Protection](#).

Scan a File When:

Run: Scans a program file each time you run it.

Opened: Scans files whenever they are opened, such as when you copy a file.

Created: Scans files when they are created on your drive by an installation program, by compressing or uncompressing a file, or by some other means.

What to Scan:

All Files: Scans all files you access. This includes files less likely to contain viruses.

Program Files Only: Scans files with the extensions contained in the program file extensions list. These are the files most likely to be infected.

Program Files button: Takes you to the [program file extensions](#) list, where you can see, add, or delete file extensions.

When a Virus is Found:

Prompt: Informs you when a known virus is found and allows you to choose how to respond.

Deny Access: Prevents you from using a file when a known virus is detected.

Repair Automatically: Repairs an infected file or boot record without notifying you. The outcome of the repair is recorded in the activity log. Note that, by default, Norton AntiVirus makes backup copies of files before they are repaired. See [General Settings Reference](#) for more information.

Delete Automatically: Deletes an infected file as soon as a known virus is detected. The name of the deleted file is recorded in the activity log.

Halt Computer: Halts your computer when a known virus is detected. You must then restart your computer.

Buttons to Display if Prompted:

Repair: Allows you to repair the file.

Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is dimmed.

Continue: Allows you to continue accessing the file. If you select the Continue button when a virus is found, you may activate the virus.

Stop: Allows you to stop accessing the file. The virus will not be activated, but the file will still be infected.

Exclude: Allows you to exclude the file from being checked for known viruses. (Use sparingly!)

Other Settings:

Advanced: See [Auto-Protect Advanced Settings](#)

Startup: See [Auto-Protect Startup Settings](#)

Sensor: See [Auto-Protect Virus Sensor Settings](#)



Auto-Protect Advanced Settings

Use these settings to have Norton AntiVirus check for virus-like activities and scan floppy disks for boot viruses before using them.

Virus-Like Activity Monitors

These settings determine what Norton AntiVirus does when it detects each virus-like activity. For each activity, your choices are:

Allow: Allows the activity to continue every time without informing you. Selecting Allow offers you no protection against an unknown virus performing that activity.

Prompt: Informs you when a program tries to perform the activity and allows you to decide whether the activity should continue, stop, or be excluded for the program. This choice provides you with the best combination of flexibility and protection.

Do not Allow: Prevents the activity from occurring every time it is detected. This selection provides the greatest protection, but can impede your work if you are legitimately trying to perform the activity.

Virus-Like Activities:

Low-Level Format of Hard Disk: A low-level format of your hard disk obliterates all information on the disk, and it cannot be recovered. This type of format is generally performed at the factory only. Detection of this activity almost certainly indicates an unknown virus at work.

Write to Hard Disk Boot Records: Your hard disk boot records should be written to only by very few programs. Detection of this activity often indicates an unknown virus at work.

Write to Floppy Disk Boot Records: Floppy disk boot records should only be written to by few programs. Detection of this activity can indicate an unknown virus at work.

Write to Program Files: Program files are written to by programs that save configuration information within themselves rather than in a separate file. This activity occurs legitimately more often than the preceding activities, though viruses must write to program files to infect them.

Read Only Attribute Change: Many programs change a file's read-only attribute, so this activity is least likely to indicate a virus at work. Some viruses, however, will change this attribute, so they can write their viral code to the file.

Check Floppies:

Boot viruses are most likely to spread through floppy disks, so it's important to check every floppy disk you use. Use these settings to ensure maximum safety automatically.

Check Floppies for Boot Viruses Upon Access: Checks for boot viruses on each floppy disk you access.

Check Floppies when Rebooting Computer: Checks a floppy disk in drive A: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del.

When Rebooting, Check Both Drives

(A: and B:): Also checks a floppy disk in drive B: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del. Check this option if you have a system that can boot from a disk in your B: drive.

CAUTION: These last two options do NOT offer protection when you restart your computer using the power switch or Reset button.



Auto-Protect Startup Settings

Use these settings to define what automatic protection does when you start up your computer.

What to Scan Upon Startup (We recommend that you check all of these items.)

Memory: Scans for any viruses resident in your computer's memory. A virus found at this point would indicate an infection in one or more programs run prior to the time that the automatic protection feature is loaded.

Master Boot Record: Scans for boot viruses in the master boot record.

Boot Records: Scans for boot viruses in the boot records on your hard disk.

Bypass Keys

TIP: To bypass the automatic protection feature, press and hold both of the specified keys during the entire boot process.

This specifies the keystroke combination you want to use to prevent automatic protection for DOS from loading at startup. The options are: **None, Both Shift Keys, Both Alt Keys, Both Ctrl Keys.**

If you do **not** want to allow the automatic protection feature to be bypassed, select None.

WARNING: If you are using MS-DOS 6.0, do not select the Both Shift Keys option. It will cause both the CONFIG.SYS and AUTOEXEC.BAT files to be bypassed completely.

Check **Auto-Protect Can Be Disabled** to make the automatic protection feature unloadable, for example, if you need to run programs that might conflict with Norton AntiVirus. For information on how to unload the TSR, see "Unloading Automatic Protection" in the printed manual.

Check **Hide Icon In Windows** if you do not want the Norton AntiVirus Auto-Protect icon displayed on your Windows desktop.



Scanner Settings Reference

Use these settings to customize the way Norton AntiVirus scans for viruses when you initiate scans.

What to Scan...(We recommend you check all of the first three items: Memory, Master Boot Record, and Boot Records.)

Memory: Checks for viruses resident in your computer's memory. If a virus is in memory while you are scanning, every file scanned can become infected.

Master Boot Record: Checks for boot viruses in the master boot record of your hard disk.

Boot Records: Checks for boot viruses in the boot records on your hard disk and on any floppy disk that you scan.

All Files: Scans all files on your disk. This includes files that are less likely to contain viruses.

Program Files Only: Scans files with the extensions contained in the program file extensions list. These are the files most likely to become infected.

Program Files button: Takes you to the [program file extensions](#) list, where you can see, add, or delete file extensions.

Within Compressed Files: Scans files compressed using the PKZIP utility.

When a Virus is Found:

Prompt: Informs you when a virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.

Notify Only: Informs you when a virus is found, but does not allow you to repair or delete the infected file.

Repair Automatically: Repairs an infected file or boot record as soon as a virus is detected. You are informed of the results at the end of the scan.

Delete Automatically: Deletes an infected file as soon as a virus is detected. You are informed of the deletion at the end of the scan.

Halt Computer: Halts your computer when a virus is detected. You must then restart your computer.

Buttons to Display if Prompted:

If you select the Prompt setting above, you can select from these options in the group box:

Repair: Allows you to repair the file or boot record. If the virus infects an item that cannot be repaired, such as a compressed file, the button is dimmed.

Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is dimmed.

Continue: Allows you to continue scanning without resolving the problem. (This button only appears if you use the Immediate Notification option.)

Exclude: Allows you to exclude the file from being checked for known viruses. (Use sparingly!)

Advanced... button: This contains more options, including network scanning, immediate notification when a virus is found, and drive preselection. For additional information see [Scanner Advanced Settings](#).



Scanner Advanced Settings

Use these settings to further customize the way Norton AntiVirus scans for viruses when you initiate scans.

Advanced Settings...

Allow Network Scanning: Allows Norton AntiVirus to scan entire network drives. (This can be very time-consuming.)

Allow Scanning To Be Stopped: Enables the Stop button in the Scan Progress dialog box, allowing you to stop a scan in progress.

Immediate Notification: Displays an alert box whenever a problem is detected while scanning. This allows you to respond immediately, without waiting until the scan is completed.

Preselect at Start...

All Floppy Drives: All floppy drives are automatically selected to be scanned when you start Norton AntiVirus.

All Hard Drives: All hard drives are automatically selected to be scanned when you start Norton AntiVirus.

All Network Drives: All network drives are automatically selected to be scanned when you start Norton AntiVirus. (You must have checked Allow Network Scanning before you can scan network drives. Your network access privileges will affect the drives on which you may repair and delete files.)



Creating Setup Files for Workstations

Before Norton AntiVirus is installed on users' workstations you must specify global configuration options.

To create a new setup file:

- 1 Choose **New Setup** from the File menu.
All of the options return to their default settings. "(Untitled)" appears in the title bar of the Network Manager window.

To edit an existing setup file:

- 1 Choose **Open Setup...** from the File menu. The Open Setup File dialog box appears.
- 2 Select the setup file you want to edit using the list boxes.
- 3 Select OK.

The name of the setup file you selected appears in the title bar of the Network Manager window.

TIP: You may want to create a master setup file that covers the needs of the majority of your users. You can then modify the master file and use the Save Setup As... command in the File menu to save the modified file under a new name.



Customizing Installation

Use the procedures below to customize how the Norton AntiVirus Network Manager installs Norton AntiVirus on workstations.

To customize installation options:

- 1 Choose **Options...** from the Tools menu.
The Options dialog box appears.
- 2 Find and select the Install/Update category on the left side of the Options dialog box.
The Options - Install/Update Settings dialog box appears.
- 3 Type the network path that contains the Norton AntiVirus files in the **Network Directory To Install From** text box.
Use the server name and path, not drive letters. For example, on a Novell network a valid pathname might be \\SERVER1\SYS:PUBLIC\NAV.
Or,
Select the browse button to see a dialog box from which you can choose the network path.
NOTE: You do not normally have to select anything because your current directory is the default. You do not have to specify the current directory.

- 4 Specify in the **Local Directory to Install To** group box where you want Norton AntiVirus installed on the workstation.
Use Previous Directory: Overwrite an existing version of Norton AntiVirus if found on the workstation. (This option assumes the Norton AntiVirus directory is in the workstation's PATH statement).
If a previous version of Norton AntiVirus is not found, the user is either prompted for a location or Norton AntiVirus is installed into the directory specified in the Use Default text box (depending on which other option is selected).
Prompt: Lets the user decide where to install Norton AntiVirus. The text entered in the Use Default text box is offered to the user as a default selection.
Use Default: Installs Norton AntiVirus to the drive and directory you specify in the text box.
- 5 Specify what to add to the workstation's AUTOEXEC.BAT file.
Run NAV.EXE: Causes Norton AntiVirus to scan the users workstation each time it starts up.
Add NAV Directory To Path: Adds the pathname where Norton AntiVirus resides to the workstations search path.
- 6 Select an option from the **Auto-Protect** drop-down list box to specify how you want automatic protection set up on the workstation.
Do not Install: Does not add the automatic protection feature to the workstations startup files. Selecting this option reduces the level of protection on the workstation.
Install in CONFIG.SYS: Adds the automatic protection feature command line to the workstations CONFIG.SYS file. The automatic protection feature will load as a device driver.
Install in AUTOEXEC.BAT: Adds the automatic protection feature command line to the workstations AUTOEXEC.BAT file. The automatic protection feature will load as a TSR (terminate-and-stay-resident program).
Note that the only way automatic protection can be unloaded is to configure it to be unloadable and to load it as the last TSR in memory.
- 7 Check **Retain Settings When Updating** to prevent updating users' configuration

settings when updating the Norton AntiVirus executable files or virus definition files. Note that this does not apply when updating from versions previous to Norton AntiVirus 3.0.

- 8 Check **Force Logoff If Auto-Protect Not Installed** to prevent users from logging onto the network when the automatic protection is not enabled on their workstations.

NOTE: Do not check this option if you selected Do not Install in step 6. Doing so will always prevent the user from logging onto the network.

- 9 Check **Confirm All Prompts** to allow users to verify information they enter for user registration and the directory to install to.



Setting Pre- and Post-Install Actions

You can specify what actions should occur on a workstation before and after Norton AntiVirus is installed.

To set pre- and post-install actions:

- 1 Select **Before...** in the Options - Install/Update Settings dialog box. The Before And After Installing/Updating dialog box appears.
- 2 Specify the areas on the workstation that should be scanned before Norton AntiVirus is installed.
 - Scan Memory:** Scans the workstations random access memory for viruses.
 - Scan Hard Disk System Areas:** Scans the workstations hard disk boot records for viruses.
 - Scan Program Files:** Scans all program files on the workstations hard disk.
 - Scan Always:** Scans the workstation every time it logs onto the network. The areas scanned are determined by the other options you selected in this step.
- 3 If you want a specific program to run *before* Norton AntiVirus is installed on the workstation, type the command in the **Command To Execute Before Install/Update** text box or select the browse button to choose a command.
Check **Execute Command Always** to launch the program every time the workstation logs onto the network.
- 4 Select an option in the **Action** drop-down list box that specifies what to do after the installation is complete.
 - Prompt to Reboot:** Prompts the user whether to reboot or not.
 - Do not Reboot:** Does not restart the workstation after Norton AntiVirus is installed. Automatic protection will not be enabled or updated until the next time the user restarts the system.
 - Reboot:** Restarts the workstation automatically after Norton AntiVirus is installed.
- 5 If you want a specific program run after Norton AntiVirus is installed on the workstation, type the command in the **Command To Execute After Install/Update** text box or select the browse button to choose a command.
Check **Execute Command Always** to launch the program every time the workstation logs onto the network.
- 6 Select OK.



Customizing User Registration

Every installed copy of Norton AntiVirus should be registered. You can specify standard information for all workstations, or let users respond to registration prompts during installation.

To customize user registration:

- 1 Select **User...** in the Options - Install/Update dialog box.
The User Registration dialog box appears.
- 2 Specify the method for registering the software.
Prompt: Prompts the user to enter the company name. If you enter text in the Use Default text box, it is offered to the user as a default selection.
Use Default: Uses the company name you enter in the text box.
- 3 Check **Prompt for Name** to prompt the user to enter his or her name.
- 4 Select OK.



Setting Additional Windows Options

For those users who work with Windows, you can further configure the installation program to install Norton AntiVirus for Windows.

To customize Norton AntiVirus for Windows install:

- 1** Select **Windows** in the **Options - Install/Update Settings** dialog box.
The **Windows** dialog box appears.
- 2** Check **Install NAV for Windows** to install Norton AntiVirus for Windows on workstations.
- 3** Check **Load Windows Drivers** to install automatic protection for Windows.
- 4** Check **Create Windows Group** to create a new Windows group on the workstation called "Norton AntiVirus."
- 5** Select **OK** in the **Windows** dialog box.
- 6** Select **OK** in the **Options - Install/Update Settings** dialog box.



Saving Your Changes to a Setup File

To save settings to a setup file:

- ◆ Choose **Save Setup** from the File menu.
If you did not name the setup file previously, you are prompted for a name.

To save settings to a new setup filename:

- ◆ Choose **Save Setup As** from the File menu.
A dialog box appears where you can type the name of the new setup file or select an existing file to overwrite.



Updating a User's Login Procedure

To install Norton AntiVirus on a workstation, you must modify the user's login procedure (the login script or batch file) to include NAVUPDTW.EXE, which is the program that installs or updates Norton AntiVirus, and the name of the setup file. If you do not specify a setup filename, default settings are used.

The next time the user logs onto the network, Norton AntiVirus will be installed. Subsequently, when new versions of Norton AntiVirus or new virus definitions files are installed on the network, the workstations will get updated as well.

Contents of Setup File

For your reference, each command added to the setup file is explained in the NAVNET.TXT file. The Norton AntiVirus setup file (.NNS file) options are generally set through the Network Manager; however, you can also edit the setup file directly using a text editor.



Auto-Protect Virus Sensor Settings

Use Virus Sensor Technology

Check this option to use the full power of Norton AntiVirus to detect unknown viruses.

When an Unknown Virus is Found:

Prompt: Informs you when an unknown virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.

Repair Automatically: Repairs an infected file as soon as an unknown virus is detected. The repair is recorded in the activity log.

Delete Automatically: Deletes an infected file without asking you. The deletion is recorded in the activity log.

Halt Computer: Halts your computer when an unknown virus is detected. You must then restart your computer.

Buttons to Display if Prompted:

If you select the Prompt setting above, you can select from these options in the drop-down list box:

Repair: Allows you to repair the file.

Delete: Allows you to delete the file.

Continue: Allows you to continue working. The file is still infected with the unknown virus.

Exclude: Allows you to exclude the file from being checked for unknown viruses. (Use sparingly!)



Keyboard Shortcuts

The following key combinations activate corresponding Norton AntiVirus functions and commands:

Menu Command Keys

Use these keys to select and execute corresponding menu commands.

Keys	Menu Command
Alt or F10	Selects the first menu on the menu bar.
Alt + underlined letter	Selects the menu whose underlined letter matches the one you press.
Underlined letter	When in a menu, selects the command whose letter matches the one you press.

Mouse Equivalent Keys

Use these keys to navigate Norton AntiVirus without a mouse.

Keys	Movement
Up Arrow	Moves up one item or line in a list or text box. Or moves among menu items in a selected menu.
Down Arrow	Moves down one item or line in a list or text box. Or moves among menu items in a selected menu.
Left Arrow	Moves left one character in a text box. Or moves left among menus.
Right Arrow	Moves right one character in a text box. Or moves among menu items in a selected menu.
Alt + underlined letter	Moves to the option or group in a dialog box whose underlined letter matches the one you press.
Underlined letter	Executes the command (in an open menu or dialog box) whose underlined letter matches the one you press.
Tab	Moves right one character in a text box. Or moves among menu items in a selected menu. Or moves between dialog box elements.
Shift + Tab	Moves up one item or line in a list or text box. Or moves among menu items in a selected menu. Or moves backward between dialog box elements.



Credits

Software Development

Jonathan Allee, Jim Belden, Tim Cashin, Mark Zaremba.

Quality Assurance

Kerry Boyte, Paul Davis, Craig Lance, Rion Millen, Howard Mora, Greg Patterson, Scott Smith

Product Management

Lily De Los Rios, Sharon Ruckman

Documentation and On-line Help

Elizabeth Anders, Karen Goldsmith, Robert Hoffman, Robert Squires

Technical Support

Christine Frazer, Todd Kieser, Michael Logue

Engineering Services

Frank Arjasbi, Steve Blackmoore, Jennifer Brawer, Annette Brown, Alfred Ghadimi, Romey Keys, Sheelagh O'Connor, Vickie VonBergen

Configuration Management

Justin Chang, Renal Fuller, Helen Kim

External Test

Erick Bryant, Richard Espy, Will Jobe, Bob Kirwin

SARC

Diop Bankole, Frank Barajas, Matt Candeleria, Philip Debats, Tigran Khanpalyan, Maryl Magee, Charles Renert



Program File Extensions

Program files are the files most likely to become infected and spread viruses. When you configure Norton AntiVirus to scan program files only, it looks at the program file extensions list and scans only files with extensions in the list.

Use the Program File Extensions dialog box to add new extensions, to delete extensions, and to reset the extensions to the original list installed with Norton AntiVirus. The list contains the most common extensions for executable files. A file must be executable for a virus to spread from it.

Add...: Allows you to add an extension (you'll be prompted to type the extension's letters).

Delete: Deletes the extension you've selected in the list.

Default: Resets the extensions to the original list installed with Norton AntiVirus.



Open Setup File

Select a setup file from the list box, or type the name of a new one, then select OK. The default setup filename is `_DEFAULT.NNS`.

A setup file contains the settings for installing, updating, and using Norton AntiVirus on a workstation. You can create one setup file for everyone to use, or you can create different setup files for different groups of users.

TIP: It's a good idea to create one "master" setup file that you can then modify, using the Save As... command in the File menu to save the modified file under a new name.

See also:

[Install/Update Settings Reference](#)



Save Setup File As

Use this dialog box to name a new setup file or to save an existing setup file with a different name. Type the new name for the setup file and select OK.



Add Program File Extension

Type a new extension in the **Extension to Add** text box (up to three characters). You may use wildcards in the extension, but not to represent all three characters.

This new extension is added to the program file extensions list, and Norton AntiVirus will treat any files with this extension as program files when it scans for viruses and inoculates.



Activity Log Filename

Select an activity log file and select OK.

File Name: Type the path and filename if you know it; otherwise select the drive, directory, and file type from the other list boxes, then select the file from the list box.

Drives: The drive shown in the window is selected; to select a different drive, use the drop-down list box.

Directories: Select a directory.

List Files of Type: Select the type of file in the drop-down list box. All files of the selected type will appear in the File Name list box.



Command to Execute Before or After Install/Update

Select a file to run and select OK.

Filename: Type the path and filename if you know it; otherwise select the drive, directory, and file type from the other list boxes, then select the file from the list box.

Drives: The drive shown in the window is selected; to select a different drive, use the drop-down list box.

Directories: Select a directory.

List Files of Type: Select the type of file in the drop-down list box. All files in the directory of the selected type will appear in the File Name list box.



Network Directory to Install From

Select the directory that contains the setup files and Norton AntiVirus files and select OK.

NOTE: You do not normally have to select anything because your current directory is the default. You do not have to specify the current directory.

Drives: The drive shown in the window is selected; to select a different drive, use the drop-down list box.

Directories: Select a directory.



Viewing the Exclusions List

Norton AntiVirus uses the entries in the exclusions list in all scans it performs. An exclusion is a condition or activity that would normally be detected during a scan, but you have told Norton AntiVirus not to look for in a particular file.

To view the exclusions list:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Exclusions List category on the left side of the Options dialog box.
The Options-Exclusions List Settings dialog box appears.
- 3 Select a file or group of files in the **Items** group box.
The activities excluded for the file or files are displayed in the **Exclusions** group box.
- 4 Select OK.



Modifying the Exclusions List

Adding Exclusions

In most cases, you add an exclusion when you select the Exclude button to resolve a problem that Norton AntiVirus has detected. You can also add exclusions to Norton AntiVirus manually.

To add exclusions manually:

- 1 Select **Add...** in the Options - Exclusions List Settings dialog box. The Add Exclusion dialog box appears.
- 2 Type the pathname for the file or group of files in the **Item** text box.
Or,
Select the **Item** browse button to choose a single file from a list, then select OK.
If you enter a filename with no path, such as NAV.EXE or JUNK.*, all files fitting that description are excluded.
If you enter a full pathname, such as C:\NAV\NAV.EXE or C:\JUNK.*, only files in that directory fitting that description are excluded.
If you enter a directory, all files in the directory are excluded.
- 3 Check **Include Subdirectories** if you want files in the subdirectories of the item to be excluded also. Note that this option only applies if the item is a directory.
- 4 Check the activities that you want Norton AntiVirus not to look for in the item specified. For a list, see [Add/Edit Exclusion](#).
- 5 Select OK in the Add Exclusion Settings dialog box.
- 6 Select OK in the Options - Exclusions List Settings dialog box.

Editing the Exclusions List

You can edit the exclusions list when changes are necessary.

To edit the exclusions list:

- 1 Select a file or group of files in the **Items** group box in the Options - Exclusions List Settings dialog box.
- 2 Select **Edit....** The Edit Exclusion dialog box appears.
- 3 Change the appropriate settings.
- 4 Select OK in the Edit Exclusion dialog box.
- 5 Select OK in the Options - Exclusions List Settings dialog box.

Deleting Exclusions

If you no longer want to use an exclusion, you can delete it.

To delete an exclusion:

- 1 Select a file or group of files in the **Items** group box in the Options - Exclusion List Settings dialog box.
- 2 Select **Delete**.
The exclusion is deleted from the list.
- 3 Select OK.

Be sure to reload automatic protection to activate the new settings.



Select Network Users

To send messages from Norton AntiVirus to other users on your network, select the Server, the Type, and the names of those available from the lists.



About...

This command displays information about the product version.



Verify Password

Type your password to access the feature.



How to Use Help

This command displays information on how to use the Windows help system.



What Network Manager Does

Network Manager provides a fast and easy way to configure and distribute Norton AntiVirus to workstations running under DOS and Windows 3.x. You can use Network Manager to perform the following tasks:

- ◆ Automatically distribute new and updated installations of Norton AntiVirus for DOS/Windows 3.x and virus definitions file updates to workstations
- ◆ Customize how Norton AntiVirus is installed to workstations
- ◆ Scan each target workstation's memory and hard disk for viruses before installing
- ◆ Customize how Norton AntiVirus behaves on workstations
- ◆ Control Norton AntiVirus TSRs (terminate-and-stay resident programs)
- ◆ Run batch files before or after an installation or update to accommodate special commands and processes.
- ◆ Enforce Norton AntiVirus Auto-Protect usage on workstations.



How Network Manager works

Network Manager includes Norton AntiVirus for DOS/Windows 3.x files and an engine that distributes Norton AntiVirus to DOS and Windows 3.x workstations. You install both the Norton AntiVirus files and the distribution engine on a server.

You use a default or customized setup file that contains information Network Manager uses to install and configure Norton AntiVirus on each workstation. (You can create multiple setup files to accommodate different workstation hardware and software configurations, and to allow for variations on how Norton AntiVirus behaves on different workstations.)

The Network Manager program, NAVUPDTW.EXE, installs or updates Norton AntiVirus on workstations based on the contents of the setup file.

By adding a command line to your users login procedures, you enable Network Manager to install and continually update all workstation copies of Norton AntiVirus for DOS/Windows 3.x. When a workstation logs onto the network, Network Manager verifies that the workstation is using the most recent version of Norton AntiVirus and virus definitions files, and that the most recent configuration settings are being used. If the Norton AntiVirus configuration settings on the workstation do not match those in the setup file on the network, the workstation settings are updated. See the printed documentation for a description of all Network Manager Components.



Using Intelligent Updater

While using LiveUpdate provides you with a fast and easy way to update your virus definitions files, you can use also Intelligent Updater. Intelligent Updater is an executable file that contains the latest virus definitions files.

The latest Intelligent Updater file is always available for download from the following sources:

- ◆ Symantec World Wide Web site
Connect to <http://www.symantec.com/avcenter/index.html>, then click Download Updates.
- ◆ Symantec FTP site
Connect to <ftp.symantec.com/public>, or click the FTP button at the bottom of any Symantec Web page.
- ◆ CompuServe
Go SYMNEW, then search the Norton AntiVirus library.
- ◆ America Online
Keyword: SYMANTEC
- ◆ Symantec BBS
To connect to the Symantec BBS, call (503)484-6669. Follow the prompts to login, then choose [G]et a File from the main menu, and then choose [G]et the latest definition file. Follow the prompts to download.

To update the definitions with Intelligent Updater, download the executable file to a temporary directory, such as C:\TEMP, then run the executable.

To run Intelligent Updater:

- 1** Download the file to a temporary directory, such as C:\TEMP.
- 2** From File Manager, double-click the filename.
For example, if you downloaded the December 1997 definitions, double-click 12NAV97.EXE.
The Intelligent Updater opening screen appears.
- 3** Click Yes and follow the prompts to update the definitions.

NOTE: We recommend that when you update the virus definitions, that you do so both in the Norton AntiVirus program folder *and* on the Norton AntiVirus Rescue Disk set.



Educating Your Users

Conduct an informational meeting with your network users to discuss the basic nature and behavior of computer viruses. Stress that while having a computer virus on your system is reason to take immediate action, there is no need to panic. Emphasize that many viruses spread from illegal or bootlegged software copies, and prohibit their use in your organization. Finally, explain how youve configured Norton AntiVirus to respond to a virus.

Instruct your users to:

- ◆ Scan all software before using it. This includes programs downloaded from electronic bulletin boards and new software right out of the shrink-wrapped box.
- ◆ Watch for warning signs, such as frequent system crashes, lost data, screen interference, and suddenly unreliable programs.
- ◆ Keep a current store of virus-free program backups.
- ◆ Avoid running programs from floppy disks they have not scanned.
- ◆ Write-protect their floppy disks before using them in someone else's computer.
- ◆ Avoid leaving a floppy disk in drive A: when rebooting the computer (to prevent the spread of a boot virus).



Staying Protected

To protect the workstations:

- ◆ Scan each workstation to make sure it is virus-free.
- ◆ Create and write-protect a rescue disk for each workstation and store it in a safe place. Update the rescue disk whenever there is a hardware configuration change.
- ◆ Train your users to use a file backup utility on a regular basis.
- ◆ Regularly update the network copies of the virus definitions files for Norton AntiVirus. Be sure that you keep current on all anticipated viruses and be prepared to prevent them.

To protect the network:

- ◆ Password protect all network executable directories so that only you can access them.
- ◆ Scan for viruses on new and rental computers before using them.
- ◆ Set up Norton AntiVirus to send an alert message to your computer's console automatically if a virus is detected on a workstation.
(If you also use Norton AntiVirus for NetWare, the alert can be sent to your pager or via electronic mail!)

To responding to a viral infection:

- ◆ Physically disconnect the workstation from the network. Then eradicate the virus on the workstation before reconnecting to the network.
- ◆ Notify other users on the network to scan for viruses immediately.
- ◆ Scan your network servers for viruses.

NOTE: If you suspect that you have an unknown virus, you can submit to the Symantec AntiVirus Research Center (SARC) for analysis. See the Potential Virus Submission Procedure form in the back of the Administrators Guide for more information.



Troubleshooting

This section explains how to resolve some common problems that may arise when you are using Network Manager. Follow the suggestions and procedures provided here before calling Symantec Technical Support.

NAVNET will not install correctly

If NAVNET does not install correctly, check for the following:

Your network drive mapping is correct; you are not using the UNC for the network location.

- ◆ The specified path is accurate
- ◆ You do not have write access to the location to which you are installing
- ◆ There are no typographical errors in the NNS file.
- ◆ Mismatched dates
- ◆ Your custom NNS script has not become corrupted.
- ◆ All section headings in _DEFAULT.NNS are also present in your custom NNS file.

Network installation directory

When editing the NNS file through NAVNETW.EXE, a pathname similar to the following appears:

\\SERVER \Public\Apps\NAVNET. (This is a pathname.)

The **Network Directory to Install From** option may not work with all versions of DOS if you select a UNC path name. If it does not, do this:

- 1 Open the NNS file with a text editor:
- 2 In the NetworkDir= parameter of the [Install/Update] section, delete any characters following the equal sign (=).

The login script already points to the directory on the server.

NNS file and NAVUPDTW.EXE version numbers must match

If you upgrade NAVNET (for example, with UPDATEME.EXE), verify that the NNS file and NAVUPDTW version numbers match in any custom NNS files you created. To verify the version numbers:

- 1 Open the new _DEFAULT.NNS file with Network Manager.
- 2 Save the new _DEFAULT.NNS file with the same filename of your custom NNS file.
- 3 Overwrite the old NNS file.
- 4 Edit the new NNS file with your selections and options.

Preparing for Shared Windows installs

Before you run a shared Windows install, do this:

- 1 Copy SYMEVNT.386 and SYMEVNT1.DLL to the Windows subdirectory on the server.
- 2 Check that the path statement in the AUTOEXEC.BAT file of the workstation has the subdirectory containing the user's SYSTEM.INI, WIN.INI, and WIN.COM before the directory of the shared network copy of Windows on the server.

Note: When Network Manager searches for and tries to modify the SYSTEM.INI and WIN.INI, it searches the Search Path as shown when you enter PATH or MAP (in Novell). However, it looks for WIN.COM. If it is not found, Network Manager stops without modifying the SYSTEM.INI in the SERVER\VOL:Subd\Users subdirectory, even if it finds the user's subdirectory before the Windows executable subdirectory.

NAVUPDTW install fails with read error

Problem: You updated Network Manager or the virus definitions files on a Novell NetWare server. NAVUPDTW reports read errors when trying to install to or update a workstation unless the user's rights to the NAVUPDTW directory are set to ALL.

Solution: Scan from within the Network Manager directory immediately after updating the definitions. To scan:

- 1 Log in as supervisor.
- 2 Change to the Network Manager directory.
- 3 Type DEL IN*.DAT and press Enter.
- 4 Type NAV . and press Enter. (Be sure to include the period, preceded by a space, to scan the current directory.)

NAVUPDTW does not reboot

Problem: Youve made changes in your NNS file for NAVUPDTW. When NAVUPDTW re-runs and makes changes, the workstation does not reboot, even though you enabled the Network Manager option to reboot when changes are made.

Solution: You must make a change in the NNS file that will affect the NAVTSR. If you have not made changes to the NNS file that will affect the NAVTSR, the workstation will not reboot.

NAVUPDTW fails during login

Problem: You are trying to run NAVUPDTW.EXE from the login script and get an Unable to read or Insufficient memory error message.

Cause: LOGIN.EXE always swaps to extended or expanded memory when running an external command unless the command Noswap is specified on the command line or in the login script. Noswap prevents LOGIN.EXE from being swapped out of conventional memory. Then, if the workstation does not have enough memory to handle both login and the external command (NAVUPDTW.EXE in this case), the external command fails but the rest of the login script executes.

Solution: Edit your setup file. Look for and remove a line with the command Noswap.

Memory issues

NAVUPDTW requires 185K. If memory problems occur, try creating a batch file called NAVSTART.BAT. Edit the batch file so that it contains the following lines:

```
Map Root L:=Sys:Public\NAVNET
```

```
L:
```

```
NAVUPDTW Filename.nns
```

```
Map Del L:
```

```
Win (or any other DOS application you might want run)
```

```
Novell exits the login script, then begins the batch file. The batch file instructs NAVUPDTW to use the <Filename>.NNS file to install Norton AntiVirus onto the local workstation.
```

Normally, any external command run from within a Novell login script forces the entire login script to be cached into the memory of the workstation while the external command runs. The script then reloads and finishes running. The memory requirement for caching the script can be as much as 100K. This can cause memory errors on the workstation that is logging on. By using the Exit command, the batch file runs after the login script.

The disadvantage of this process is that any User Login Scripts will not run after the Exit

command.

Problem: You run NAVUPDTW from the login script and receive memory errors, an EMM386 exception error, and/or lock up.

Solution: Complete the following steps:

◆ Enter the following at the top of the login script:

Map Root G:=sys:NAVNET (or directly to the sub-directory that contains the NAVNET files.)

#G:\navupdtw (or #G:\navupdtw filename.nns if you are not using the default filename. Filename is the name of your nns script file.)

Map Del G:

Alternatively, you can create a batch file, NAVSTART.BAT, and call it from the login script after the EXIT command. NAVSTART.BAT contains the following:

N: enter (change to the mapped network drive where Navupdtw is located)

CD\path to navupdtw

navupdtw (or navupdtw filename.nns if you are not using the default nns script filename.)

Any other startup batch files

The last line is:

EXIT

or

EXIT NAVSTART.BAT

Add NAVSTART.BAT (with quotes) to the EXIT line if you want to run the batch file at the end of the login script. If you add NAVSTART.BAT, it must appear on the EXIT command line because Novell uses 90K of conventional memory when you run a DOS file from within the login script, unless you run it immediately after exiting the script.

NAVUPDTW hangs on a system with Disk Manager

NAVUPDTW hangs when run from the login script on a system with Disk Manager when NAVUPDTW and Disk Manager are attempting to use the same region of memory. To resolve the conflict:

- 1 Load DM.EXE from the Disk Manager disk.
- 2 Select the Maintenance Menu option.
- 3 Select the Update Menu option.
- 4 On the only line on the screen, type the following

/L=0

(/L=Number zero)

This switch enables you to turn off the memory redirection to the upper memory range for Disk Manager where NAVUPDTW is loading.

Distributing in a shared Windows environment

Problem: When you run NAVUPDTW under a shared Windows environment, the message Error modifying Files appears on one or more workstations when you run any NNS file.

Cause: NAVUPDTW fails after attempting to put its SYMEVENT files in a file named SYSTEM in the \Windows directory, mistaking this file for the Windows\System directory.

Solution: Delete any file named SYSTEM in the \WINDOWS directory, then rerun NAVUPDTW.

Situation: If your workstations use a shared installation of Windows from the network, you need to take some extra steps to ensure that NAVUPDTW copies the Norton AntiVirus Windows components to the correct location.

Solution: Follow these steps:

- 1 Copy SYMEVNT.386 and SYMEVNT1.DLL to the Windows subdirectory on the server.
- 2 Make a System subdirectory under the Windows subdirectory on the server and copy SYMEVNT.386 and SYMEVNT1.DLL there as well.
- 3 Make sure the path statement in the AUTOEXEC.BAT of the workstations have the subdirectory for C:\Windows listed before the server's Windows directory path.
- 4 If you have the workstation using a User's subdirectory on the server for the local Windows files (SYSTEM.INI and WIN.INI), make sure that it is in the path before the Shared Windows subdirectory on the server.
- 5 Edit the NNS file and set UseWinSysDir=1. If it fails, set it to =0.
- 6 Make sure WIN.COM is not named anything other than named WIN.COM (such as WIN31.COM).

Turning off NAV.EXE Color-B/W prompting

If your users must select Color or Black and White the first time they run NAV.EXE after an update, you can complete the following steps to turn the prompt off:

- 1 Run NAV.EXE from the NAVUPDTW directory.
- 2 Select Color or B/W.
- 3 Exit NAV.EXE.
- 4 Add SYMCFG.BIN to the [InstallFiles] section of the NNS file.

NetWare issues

User Cannot Log Back Into a NetWare 4.x Server

Problem: After you have run NAVUPDTW to distribute Norton AntiVirus you cannot log back into the NetWare 4.x server.

Solution: The problem is caused by a setting in Novell 4.x only which allows a user only one login at a time. You must turn off the auto reconnect setting under Novell 4.x at the workstation. To do this, edit the file NET.CFG file, which should be in the \Nwclient subdirectory. Add or change a line so it reads as follows:

Auto reconnect = Off

This line should go in the DOS Requester Adjustments section. For more information, please refer to your Novell NetWare documentation.

System hangs after the Novell NetWare drivers load

If a workstation does not boot correctly after running NAVUPDTW, or appears to hang, check the version of the Novell drivers on the workstation.

Error messages

INSCANB not Copied due to File not Found

Specifying a path in the [Install/Update] section causes this error.

Make sure all NAVNET files are in the same subdirectory. If they are, the error is probably related to the installation of the new virus definitions files.

If all procedures have been followed correctly, do the following:

- 1 Copy the entire NAVNET subdirectory to a local drive.
- 2 Delete the IN*.DAT files.
- 3 Scan a drive or directory.

4 Copy all the files back to the network directory. Overwrite them.

NAVUPDTW error levels

These DOS error levels can be returned when running the NAVUPDTW program:

Error Level	Description
0	No changes were made to Norton AntiVirus on the workstation.
1	Program files, settings, and virus definitions were installed.
2	Virus definitions were updated. Program files or settings may also have been updated.
3	Program files and/or settings were updated.
4	An error occurred during execution.
5	Execution was halted because a virus was detected on the workstation.
6	Execution was aborted by the user.
255	Workstation is not compatible with Norton AntiVirus.

