

Administration

This chapter contains information for the network administrator. It explains how to create and maintain *network groups* (application groups available to network users), and how to restrict availability of those groups, and their contents, to selected users. You will also learn how to assign restrictions and requirements to features of Applications Manager and Secure Station Tools.

As an administrator, you need to understand Applications Manager and Secure Station Tools from the user point of view before you can administer these programs on the network. These applications are described in Chapter 3, “Applications Manager,” and Chapter 5, “Secure Station Tools.”

To configure and maintain Applications Manager, you use two programs:

- Applications Manager, in Administration mode (APPMAN.EXE /A)
 - Desktop Administration (WWADMIN.EXE)

Overview of Administration

Administration is the heart of Applications Manager, giving the network administrator substantial control over user desktops. You can remove menu commands, implement workstation security, and create unique application groups for network users based on their user ID or LAN group membership.

There are two programs that you use to accomplish administration tasks, Applications Manager (in Administration mode) and Desktop Administration. All administrative functions, however, are available from Applications Manager, which starts the Desktop Administration program automatically as needed.

Applications Manager Administration Mode

In Administration mode, you create network application groups accessible to all Applications Manager users on the network. You can restrict user access to the group or its contents using the Rights button in any Properties dialog box. Administration mode is accessible to you from any workstation on the network with key combination Ctrl+Alt+A, but is protected from users by network privileges and a password, if one is set.

In Administration mode, Applications Manager maintains the following files:

- *.APP files. Network group files stored on a file server available to all users, normally in the NETTOOLS directory.
- NETMENU.INI. Contains a list of network groups and several global settings. Applications Manager creates this file when needed if it does not exist.

Administrative functions performed in Applications Manager Administration mode

| Function | Procedure |
|--|---|
| Create network application groups | File menu: New/Network Group |
| Create subgroups of network application groups | File menu: New/Subgroup |
| Create program items in network application groups | File menu: New/Item |
| Restrict user access to network groups, subgroups, or items by user ID or LAN group membership | Properties dialog box: Rights button |
| Force users to reload network groups | Administration menu: Propagate Network Groups |

Desktop Administration

Using the Desktop Administration program, you can restrict access to the features of Applications Manager and Secure Station Tools, or require certain features to be used. You can remove menu items and commands from the Applications Manager menus seen by users—for example, remove the Run command from the File menu. You can configure Secure Station Tools to require the use of Secure Station. If you then place Secure Station Tools in the Applications Manager network startup group, you have enforced workstation security.

Desktop Administration maintains the following files:

- APPMAN.WWR. Applications Manager restrictions file. Applications Manager will not start without this file.
- WWEXT.WWR. Secure Station Tools Tool restrictions file. Secure Station Tools will not start without this file.

Administrative Functions Performed In Desktop Administration

| Function | Procedure |
|---|---|
| Set administrative password | (APPMAN.WWR and WWEXT.WWR) Options menu: Change Password |
| Define startup logo display for users | (APPMAN.WWR and WWEXT.WWR) Options menu: Logo Display |
| Remove items from Applications Manager menus | (APPMAN.WWR) Options menu: Menu Bar Restrictions |
| Set user defaults for Applications Manager menu item settings | (APPMAN.WWR) Options menu: Menu Bar Defaults |
| Define Secure Station Tools defaults and restrictions | (WWEXT.WWR) Applications Manager Administration menu: Secure Station Tools Restrictions. Then Options menu: Restrictions |

Running Applications Manager in Administration Mode

Applications Manager has two modes of operation: *User mode*, the normal operating mode, and *Administration mode*, a special configuration mode used by the network administrator only. User mode is described in Chapter 3, “Applications Manager.”

To enter Administration mode:

- If Applications Manager is running in User mode, press Ctrl+Alt+A to toggle into Administration mode.

OR

- Type APPMAN.EXE /A in any File/Run command line box (in, for example, File Manager or even Applications Manager itself). If Applications Manager is not running, it starts in Administration mode; if it is already running, it toggles into Administration mode. (You cannot start a second instance of Applications Manager.)

If a password is configured, you are prompted for it. Your product is shipped without a password so there is no initial password prompt (to set one, see “Changing the Password” in this chapter). Only one user at a time may be in Administration mode.

Administration mode is identified by *Applications Manager - Administration Mode* in the title bar. The status bar indicates the network workspace (NETMENU.INI file) you are presently maintaining.

Exiting Administration Mode

Remember, in Administration mode you are editing the workspace of all Applications Manager users. Before you decide to save the changes, you should understand the ramifications of doing so—it may affect all your users. Read the section “Save Workspace” in this chapter if you have any doubts.

You can leave Administration mode in several ways:

- Choose Exit Administration Mode from the Administration menu to toggle back to User mode.
- Use the key combination Ctrl+Alt+A to toggle back to User mode.
- Type APPMAN.EXE in any File/Run dialog box (in, for example, File Manager or even Applications Manager itself) to toggle back to User mode.
- Choose Exit from the File menu to close Applications Manager (and exit Windows, if Applications Manager is your shell).

Note: If, upon returning to User mode, you find that some network groups or items do not display, it is possible that you do not have access rights to them. See “Adding Network Groups” and “Adding Network Subgroups and Items” for more information.

Using Administration Mode

This section explains how to use Administration mode to configure and maintain Applications Manager on your network.

Note: In normal operation, keep Applications Manager in User mode. Use Administration mode only for maintenance. This way you cannot disturb the network users by inadvertently saving the workspace.

Considerations

In Administration mode you are working with the *network* workspace, which all users share. Changes you make can affect all Applications Manager users on the network. This section explains some significant concepts and features that are inherent to Administration mode.

Saving Changes in Administration Mode

Before you begin adding groups and changing the network workspace, it is important to understand the nature of several commands that can affect everyone who uses Applications Manager. The two tables below summarize the various “save” commands; the following sections explain how to use them.

| File Menu Commands | Description |
|---------------------------|---|
| Save Group As | Saves the current network group file only. Because this command does not affect users until you execute a Save Workspace, it is the safe way to save changes as you go along. |
| Save Workspace | Saves changes to all network group files and NETMENU.INI. Changes are propagated to users dynamically. |
| Exit | Gives you a choice of saving workspace or forgoing all changes, then closes Applications Manager. Changes are propagated to users dynamically. |

| Administration Menu Commands | Description |
|-------------------------------------|---|
| Exit Administration Mode | Gives you a choice of saving workspace or forgoing all changes, then switches Applications Manager into User mode. Changes are propagated to users dynamically. |
| Propagate Network Groups | Forces all users to reload the network groups. |

Save Group As

Since the Save Group As command saves only the elements of a group, it is convenient to use it as you are making changes to a group and do not yet want to propagate those changes to network users. You can also save newly created groups using this command. When you are satisfied with the group or groups, you can proceed to Save Workspace as described in the next section. You can use the Print Workspace to File command to review the groups before saving the workspace.

Save Workspace

When you are satisfied with the network groups and are ready to make them available to users, select Save Workspace. This command saves any changes you have made to your network groups, including newly-created groups, and updates the NETMENU.INI file with any new groups and options.

When do users see the changes? The next time a user opens any icon, Applications Manager displays a message saying that you have changed the network groups. Then the network groups reload. They do not retain any appearance options—size, position, icon arrangement, and view type—that the user has saved. All user workspaces are rearranged to look like yours.

Automatic Icon Arrangement

If a user does not have rights to an item in a network group, the item does not display. This would appear to the user as a gap in the icon spacing. Therefore, if an icon is not displayed because of access rights, Applications Manager automatically arranges the icons within the group, filling in the gap. The user will not be aware of the process.

This feature is on by default, but you may override it. To do so, use a text editor such as Notepad to enter the following line in the [Settings] section of the NETMENU.INI file:

```
AutoArrange=0
```

Propagate Network Groups

The Administration menu offers a special command, Propagate Network Groups, that forces users to reload the network groups. Why is the command necessary? Because in User mode, Applications Manager does not reload network groups that have not been modified—even when you Save Workspace. Yet there are situations where you want users to reload the groups anyway, as in the following example.

For instance, you have assigned rights to Applications Manager network groups based on LAN group membership. The group Marketing Apps is accessible only to members of Marketing, and the group Sales Apps is accessible only to the members of Sales. This morning, an employee transferred from the Sales department to the Marketing department. Using a network utility—such as Novell's SYSCON—you change the user's LAN group membership, removing her from Sales and adding her to Marketing. However, if the user was already in Windows, she does not see the Marketing Apps network group, because she was not a member of Marketing when Applications Manager started. This is when you need to force a reload of the network groups. Applications Manager will recognize the user as a member of Marketing, and display the Marketing Apps group.

Adding Network Groups

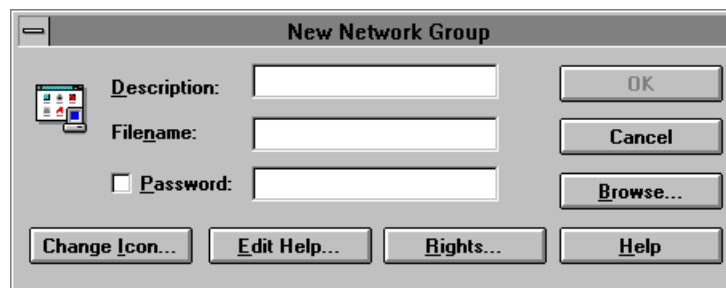
You must be in Administration mode to add network groups. By assigning rights to network groups and their contents, you can determine which groups or users on the network will have access to them. Users without access cannot open the group or item; in fact they cannot even see it. This function is accomplished entirely within Applications Manager. It is not necessary to set any file or directory permissions in the network operating system (beyond the general recommendations for this product—refer to Chapter 2, “Installation,” for more information).

Network groups cannot be modified by users; they do not have access to the New/Network Group command or to Network Group Properties.



To add a new Network Group

1. Select New/Network Group from the File menu.



2. Type the description of the new group in the text box. This will display in the group title bar. This field accepts 60 characters, but long names can clutter the desktop.

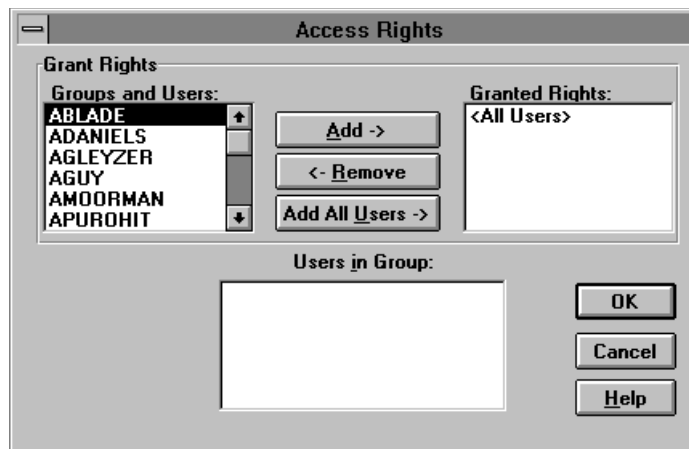
You can easily import an existing group from Applications Manager or Program Manager. See the next section, “Importing Existing Groups” for more information.

By default, Applications Manager saves network group files to its own directory. If you want to save them to another location, use the Save Group As command on the File menu followed by Save Workspace on the File menu. For more information, see the discussions above about “” and “Save Workspace.”

3. If you wish to assign a password, check the Password box and type it in the text box.

If a password is set, users must enter it to open the group. Users are not able to change the password of a network group or any item it contains. Applications Manager does not prompt for passwords in Administration mode.

4. Choose the Rights button to assign access rights to the group.



The Access Rights dialog box displays with a list box of LAN groups and users on your primary server. If you do not specify, the program default is for all users to have rights. But if you do assign rights, users—including the network administrator—who have not been granted rights to the group do not see the group icon.

Note: LAN group membership cannot be modified from the Access Rights dialog box. Use a network utility such as SYSCON for this.

5. In the Access Rights box, the Groups and Users list box shows all groups and users on your primary server, and the Granted Rights list box shows those to whom you have given access. You may give access to any combination of individual users and LAN groups. The entry <All Users> is the default in the Granted Rights box.

Select a user or a LAN group from the Group and Users list box. (If you select a group, its members display in the Users in Group list box.) Choose the Add button after each selection, or double-click on an entry, to move it to the Granted Rights list box.

The Remove button is available to remove entries from the Granted Rights list. Or, double-click on an entry to do the same thing.

6. Choose OK to assign rights and return to the New Network Group dialog box.
7. To create group-specific help, choose the Edit Help button. For information on creating help, see “Creating Applications Manager Context-Sensitive Help” in Chapter 3.
8. Choose OK again to add the new Network Group.

Importing Existing Groups

Applications Manager can easily import existing groups in the following formats:

- Program Manager groups (.GRP extension)

- Version 3 Workstation Menu groups (.DB extension), both network and personal
 - Version 4 Applications Manager groups (.APP extension), both network and personal

To import a group, select New/Network Group from the File menu. In the New Network Group dialog box, enter the full path to the group file in the Filename box, or use the Browse button to locate the group. Choose OK to exit the dialog box.

You can import all the existing group files in a directory at one time. Instead of a single filename, enter *.APP, preceded by a full path using server\volume reference or a mapped drive, to import all the Applications Manager group files in the directory at one time. This method can also import and convert all the network groups from a Version 3 installation (*.DB) or all the Program Manager files (*.GRP) in a Windows directory.

Be careful of any full paths in imported group items. The users on the network will need the same drive mappings, as discussed later in “Drive Mapping Considerations.” You can use the Print Workspace to File command on the File menu to obtain full information on the imported groups.

Network Startup Group

A startup group is a set of programs or scripts that runs each time a user starts Windows. You may wish to customize the startup group shipped with Applications Manager or create your own. To create a startup group, simply create a network group with the filename STARTUP.APP. (Users can also create personal startup groups with the filename PERSTART.APP.) Applications Manager executes startup groups, both network and personal, only if it is the Windows shell. The network startup group does not display in User mode.

Note: Setup converts the administrator’s STARTUP.GRP to PERSTART.APP so that it is not confused with the network startup file.

Adding Network Subgroups and Items

Once you have created a network group, you can add subgroups and items to it just as you would to a personal group. You may copy or move icons from other groups, or use the File menu commands New/Subgroup and New/Item.

The New and Properties dialog boxes for network subgroups and items have the Rights button, which brings up the Access Rights dialog box shown in the “Adding Network Groups” section above. You assign rights in exactly the same way, with the same results. In User mode, Applications Manager does not display the icon to users from whom you have removed access rights (which may include yourself), and automatically arranges the items in the group. Naturally, users who do not have access to a subgroup or group have no access to its contents. Users cannot access Properties of a network subgroup or item.

Drive Mapping Considerations

You can assign icons from external files to network groups, subgroups, and items. But the icon itself is not stored in the .APP file, only its source filename. If you use external icons, you should place the icon source files on the network in a directory accessible to all Applications Manager users. Because the icon filename is stored as a full path with a drive letter, users need to have the same drive mapped to this directory as you do.

The same is true if you use a full path to executables in the network items: users must have the same drive letter mapped to the volume as you do when you create the item. A better solution is to make the item run a Desktop Control Language (DCL) script; the script performs the drive mapping and adds the directory to the user's path on the fly.

In network items, the Command and Change Directory fields accept DOS environment variables. For example, if the DOS environment variable WORDPATH is set to I:\WINAPPS\WORD6, you can enter the following:

Command: %WORDPATH%\WINWORD.EXE

Change Directory: %WORDPATH%\MEMOS

Again, take care that users have the same variable defined; a DCL script can set environment variables, or you can use the DOS SET command.

Working with Other Workspaces

Administration mode includes two additional commands on the File menu, which allow you to work with other workspaces—New Workspace (cascaded from the New command) and Save Workspace As. In Administration mode, the status bar displays the workspace (NETMENU.INI location) you are currently editing.

New Workspace

New Workspace allows you to maintain another workspace, perhaps on another file server. To open an existing workspace, choose File/New/New Workspace, then select a directory and drive with an existing NETMENU.INI. Choose OK. Applications Manager loads that NETMENU.INI and the groups listed in it. You are now editing that workspace—if you add a group, it goes there, and any changes are saved there.

New Workspace can also create a new workspace. Choose File/New/New Workspace, then select a drive and directory that does not contain a NETMENU.INI and choose OK. You can now add groups to that workspace.

Save Workspace As

Save Workspace As is used to duplicate the workspace to another file server, or create a backup. Choose File/Save Workspace As, then select a drive and directory that does not contain a NETMENU.INI and choose OK. Applications Manager copies the NETMENU.INI to the directory you specified, along with all the network group files listed in NETMENU.INI. After this command, you are maintaining the new workspace, as indicated in the status bar. To go back to your original workspace, use New Workspace to open it.

If you have assigned Rights to network groups or items, take note when you save the workspace to another server. The same user ID's and Group names must exist on both servers.

Note: Use Applications Manager command Save Group As or Save Workspace As, not File Manager or DOS commands, to copy a workspace or group files. Applications Manager uses UNC (Universal Naming Convention) filenames internally in its files, which do not get modified if you just copy the files.

Printing the Workspace to a File

To keep a text record of the network workspace, select Print Workspace to File from the File menu. You can then use Notepad or a word processor to print the file.

You can select which items you want to include in the output file:

- INI files—PERMENU.INI and NETMENU.INI
- Restrictions—Menu Bar Defaults and Menu Bar Restrictions from APPMAN.WWR
 - Network groups—full information about network groups and their contents, including the Access Rights list. Does not print passwords. You can select None, all, or a specific group.

Customizing the Title Bar

The standard Applications Manager title bar is, of course, *Applications Manager*. You can specify a custom title up to 78 characters long, which will apply to all users. For example, using a text editor such as Notepad, edit the NETMENU.INI file:

```
[Title]
```

```
Title=Acme Software Company
```

Understanding Desktop Administration

Using Desktop Administration, you can restrict access to the program features of Applications Manager and Secure Station Tools, or require certain features to be used. You can remove menu items and commands from the Applications Manager menus seen by users—for example, remove the Run command from the File menu. You can configure Secure Station Tools to require the use of Secure Station. If you then place Secure Station Tools in the Applications Manager network startup group, you have enforced workstation security.

To implement the restrictions, Desktop Administration creates and maintains two *restrictions files*, APPMAN.WWR for Applications Manager and WWEXT.WWR for Secure Station Tools. These files must be located on each user's path, where the programs can read them upon startup. If either program cannot find its respective .WWR file, it will not start.

Starting Desktop Administration

Launch Desktop Administration from the Administration menu of Applications Manager (available in Administration mode only). From the Applications Manager window, use the key combination Ctrl+Alt+A to toggle into Administration mode. You must enter the password assigned to the current APPMAN.WWR file if one has been set.

From the Administration menu, choose Menu Restrictions to launch the Desktop Administration program and open the APPMAN.WWR file. Choose Secure Station Tools Restrictions to launch the program and open the WWEXT.WWR file (if that file has a password, you are prompted for it).

Alternate Method



You may launch Desktop Administration directly as a standalone program.

Choose File/Run from the menu bar in your Windows shell and enter

WWADMIN.EXE in the command line box. This method does not automatically open a .WWR file.

| |
|--|
| <p>Note: Because Desktop Administration's main window consists of only a title bar and menu bar, it stays on top of other windows so you can find it.</p> |
|--|

Creating and Editing .WWR Files

NetTools is shipped with default restrictions files, which you may open and modify. Or, you may create new .WWR files.

The commands on the Options menu correspond to the type of file you are editing, which is indicated in the title bar.



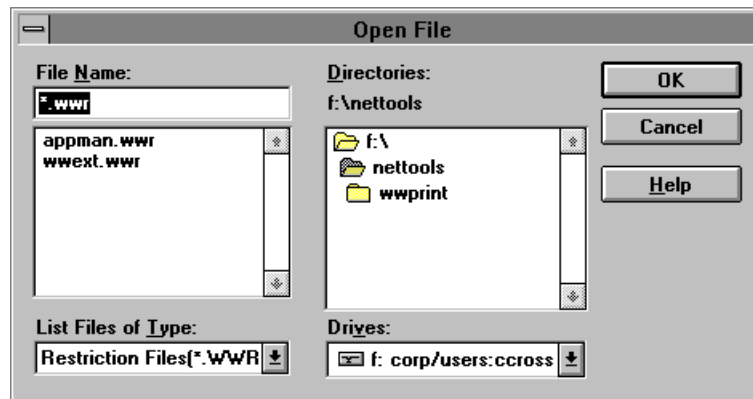
Desktop Administration window with an Applications Manager restrictions file open.

Although the Options menu varies for Applications Manager and Secure Station Tools, the procedures for defining and saving .WWR files are identical. If you work with both types of files in the same session, be sure to save your changes to one file before opening the next.



To open an existing .WWR file

1. Choose Open from the File Menu.



2. Select either the APPMAN.WWR or WWEXT.WWR file from the Files list box, changing network drives and directories if necessary.
3. Choose OK.

The Desktop Administration title bar indicates the type of file you are editing and the Options menu commands correspond to that type.

4. Enter a password if prompted for one. (If a password has not been set, you are not prompted.)



To create a new .WWR file

1. Choose New from the Desktop Administration File menu, then choose either Applications Manager or Secure Station Tools.

The title bar indicates that you are creating either an Applications Manager (APPMAN.WWR) or Secure Station Tools (WWEXT.WWR) file.

Note: If the New command is gray, you must add the [WWAdmin] section to the WIN.INI (the lines are added automatically during installation, but only to the installer's WIN.INI). The following two lines are required:

```
Applications Manager=admaman.dll
Secure Station Tools=admext.dll
```

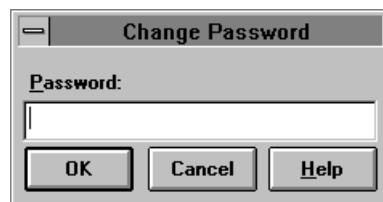
2. Set a password.

Note: The password in effect when you save a .WWR file is the one you will need next time you open it. For information on setting a password, see “Changing the Password” in this chapter.

3. Use the items on the Options drop-down menu to set restrictions for the .WWR file you are creating. (See the sections “Setting Applications Manager Menu Restrictions” and “Setting Secure Station Tools Restrictions” later in this chapter.)

Changing the Password

The APPMAN.WWR and WWEXT.WWR files shipped with the product do not have passwords. We recommend that you assign password to them to keep unauthorized users from editing the restrictions files. As an added security measure, you can move the Desktop Administration program file WWADMIN.EXE to a location inaccessible to users. The APPMAN.WWR password doubles as the Administration mode password in Applications Manager, so it is especially important.



The Change Password dialog box.

To reset the password, choose Change Password from the Options in Desktop Administrator and type your own password. Maximum password length is 31 characters.

You are prompted to type the password a second time for confirmation. Passwords, which are not case sensitive, appear “blind” for security reasons when entered in the text box.

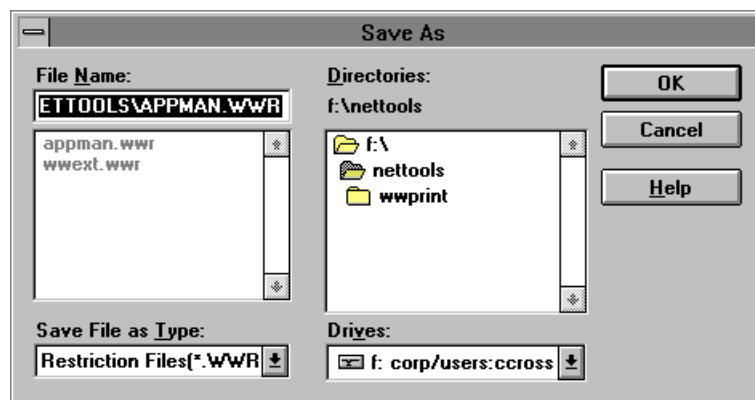
Saving .WWR Files

The procedure for saving .WWR files applies to both Applications Manager (APPMAN.WWR) and Secure Station Tools (WWEXT.WWR) restrictions files. It is important to retain the names automatically assigned to each of these files so each program can find its respective .WWR file at startup. You may want to change a .WWR filename as a temporary administrative convenience or for backup purposes. However, be sure to reassign the file’s default name when you want to use it again.



To save a .WWR file

1. Choose Save As from the File menu.



The Save As dialog box displays with the default filename and extension for the type of file (Applications Manager or Secure Station Tools) you are saving. Use the Drives and/or Directories boxes to change the drive and directory for the .WWR file’s location.

For most installations, saving the .WWR file to the NETTOOLS directory is the best choice. If you elect to keep them elsewhere, be aware that Applications Manager reads the first APPMAN.WWR file on each user’s path. Likewise, Secure Station Tools reads the first WWEXT.WWR file on each user’s path. Neither program will start without its .WWR file.

You can implement different restrictions throughout your network by creating multiple .WWR files, each including a different selection of restrictions. By placing a particular .WWR on a user's path, you determine which set of Secure Station Tools or Applications Manager options he or she can access.

2. Choose OK.

Instead of Save As, you can use the Save command from the Desktop Administration File menu to save changes to existing .WWR files.

When Do the Changes Take Effect?

Applications Manager and Secure Station Tools change dynamically according to their restrictions files; it is not necessary for users to restart the programs. Applications Manager utilizes the new settings the next time a user opens any icon in Applications Manager, displaying a message to the user that the network administrator updated some Applications Manager options. Secure Station Tools checks its restrictions file approximately once a minute, and implements any changes then.

Setting Applications Manager Menu Restrictions

As administrator, you have complete control over the configuration of the Applications Manager menu bar. You can remove any command or setting, specifying a default if necessary, to determine the way Applications Manager looks and functions for its network users. You may, for instance, restrict user access to programs by removing the Run command from the File menu.

Menu Bar Defaults

The Menu Bar Defaults dialog box lets you set default settings for selected Applications Manager menu items. If the menu item is not restricted, they are simply initial settings; a user may change them at his or her workstation. However, if the menu item is restricted, these values override any previous settings the user may have made.

Defaults for the Applications Manager menu bar can be set in three general categories:

| Category | Defaults |
|--------------|--|
| View | Horizontal Icon, Vertical Icon, and Text. |
| Options | Save Workspace on Exit, Hierarchical, Status Bar, and Minimize on Use. |
| Confirmation | Delete Group, Delete Subgroup, Delete Item, and Save Workspace. |

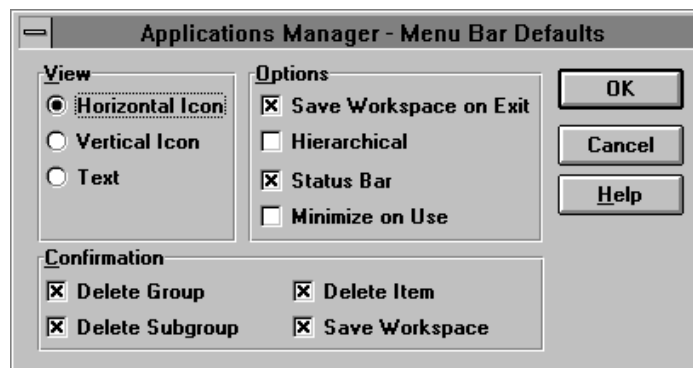
Default settings that pertain to individual windows (Horizontal Icon, Vertical Icon, and Text views, and the Hierarchical option) apply to newly created group windows. For example, if you set the default view to Text, newly created groups will be displayed in the Text view. Existing windows with other display types are not affected.

See Chapter 3, “Applications Manager” for a detailed explanation of how these menu item work.



To set menu bar defaults

1. Choose Menu Bar Defaults from the Options menu.



2. Choose items that you want as defaults by selecting a single radio button from the View group box and checking one or more of the check boxes.

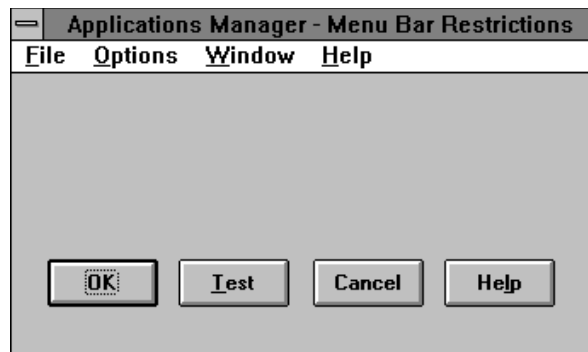
Checking an item means the default setting for that item is on (active) and it will show a check next to it on the Applications Manager menu.

3. Choose OK.

The changes take place after you save the .WWR file. See “When Do the Changes Take Effect?” in this chapter. As administrator, you see the changes as soon as you switch Applications Manager into User mode.

Menu Bar Restrictions

The Menu Bar Restrictions dialog box contains a replica of the Applications Manager menu bar for choosing the menu items that the program will display. By selecting only the menu choices you want users to have, you are able to regulate their use of Applications Manager.



The Menu Bar Restrictions dialog box initially displays in Edit mode, where check marks indicate the menu items that will display. Select an item in the drop-down menus to toggle it on (active) or off (inactive). You can view the menus as they will actually appear to users by selecting Test.

By checking an item off, you actually remove it from the users' menu bar. The command's shortcut key is disabled as well. If all of the items on a pull-down menu are restricted, the entire menu is removed from the menu bar (except the Window menu, which is never removed because it contains the window list).



To set menu bar restrictions

1. Choose Menu Bar Restrictions from the Options menu.

The Menu Bar Restrictions dialog box displays in Edit mode with a replica of Applications Manager's menu bar.

2. Choose one of the items from the menu bar.

For a new APPMAN.WWR file, the drop-down menus show all items checked on—enabled. If you are editing an existing file, the menus represent currently set restrictions. Unchecked items are restricted.

3. Check off the item that you want to remove from the menu.

Each time you check an item the drop-down menu closes, so repeat the process for each item you want to remove. Removing all items from the File/New cascaded submenu removes New from the File menu.

4. Choose Test to view a sample version of the drop-down menus you just customized. Only the items that were checked on appear in the menu now.
5. Choose Edit to return to Edit mode.
6. Choose OK if all menu bar restrictions have been set.

To edit previously set restrictions, follow the above procedure, toggling on or off the existing settings you need to change.

Considerations

- When you remove a menu item that sets a toggle—various items on the Options and Window menus—always make sure that the Menu Bar Default for the item is set the way you intend.
- When File/Run is restricted, users cannot run a program by typing the program's filename. However, it is possible to run programs using the Command feature in the Clock/Alarm Options dialog box. Alarm's Command feature may be restricted in Desktop Administration in the WWEXT.WWR file. See "Setting Secure Station Tools Restrictions" later in this chapter.
- Restricting File/Exit also restricts the System Control box for exiting Windows.
- Restricting File/Move or File/Copy also restricts the mouse drag-and-drop method of moving or copying.
 - Restricting Options/Save Workspace on Exit also disables the Save Workspace checkbox in the Exit dialog.

Logo Display

Applications Manager and Secure Station Tools display a NetTools logo during startup. You can customize the startup display, replacing the default logo with a Windows Metafile (.WMF) or a bitmap file (.BMP). Or select [None] from the drop-down list box to eliminate the logo display.

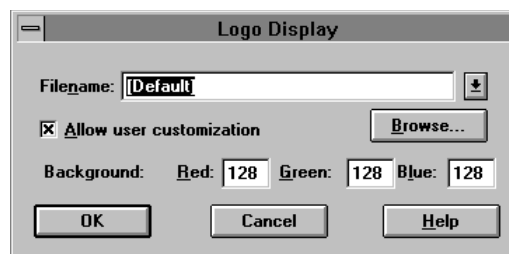
The Administration program does not check for the existence of the file you enter here so you may create it at a later time. If you don't specify a file extension, the program appends .WMF. In addition to selecting a logo, you may select the logo's background colors.

Checking the Allow User Customization check box on, when in the Logo Display dialog box, gives users the ability to change the logo file and color for their own workstation. (See the next section, "Customizing a User's Logo," to learn how a user can change the logo display.)



To change the logo display

1. Choose Logo Display from the Options menu.



2. Choose the down-arrow to select a .WMF, the McAfee default logo, or no logo from the list box.

OR

Choose the Browse button to locate another .WMF and .BMP file. Select one in the Browse Logo dialog box and choose OK.

3. Edit the logo background color by replacing the default settings with new values between 0 and 255 for each color.
4. Choose OK.

Customizing a User's Logo

If you have allowed users to customize the startup logo, they may substitute another graphics file or modify the color of the logo background that displays on their workstations. To do this, the user's WIN.INI file needs to be edited.

The Desktop logo displays for two modules: Applications Manager and Secure Station Tools. If one is already running, the other does not display the startup logo.

In the [WindowsWorkstation] section of the user's WIN.INI file, add the following parameter:

```
Logo File=<filename>
```

Replace <filename> with the name of the Windows Metafile (.WMF) or bitmap file (.BMP) that contains the user's customized logo. This file must be on the user's path.

To modify the background color of the logo display, add the following parameter to the [WindowsWorkstation] section of the user's WIN.INI file:

```
Logo Background=<Red> <Green> <Blue>
```

Replace <Red>, <Green>, and <Blue> with RGB values between 0 and 255. For a gray background, for example, enter:

```
Logo Background=128 128 128
```

Setting Secure Station Tools Restrictions

Secure Station Tools contains three utilities: Clock, Intercom and Secure Station. Desktop Administration, when editing WWEXT.WWR, lets you customize each module. You may choose to make all of them available to users, only one, or any combination. You have the ability to require Secure Station on the workstation.

In addition, you can specify a filename and color for the logo that displays at startup and allow users to customize it.

- For procedures on modifying the logo display, see the section “Logo Display” in this chapter.
- For procedures on changing the password, refer to the section “Changing the Password” in this chapter.

The Options/Restrictions menu item offers the following options:

| Module | Options | Results |
|----------------|----------------------|---|
| Clock | Enable | Checked: Clock icon displays whenever program runs. Unchecked: Clock icon does not display. |
| | Command | Checked: Users can run programs from the Alarm Options dialog box. Unchecked: Alarm can only display tickler messages. |
| Intercom | Enable Send | Checked: Users can send network messages. Unchecked: Intercom-Send icon does not display. |
| | Enable Receive | Checked: Messages icon displays when user receives a network messages. Unchecked: User does not receive network message until exiting Windows. |
| Secure Station | Enable | Checked: Secure Station icon displays. Unchecked: Secure Station icon does not display. |
| | Require | Checked: Screen Saver cannot be disabled. Secure Station Tools module cannot be closed (not even from the Task List). Unchecked: Users can set Screen Saver options as desired, and can shut down the program. |
| | Enable Messages | Checked: Leave Message feature is offered on secured workstations. Unchecked: Leave Message button is removed. |
| | Time-out range limit | Specifies minimum and maximum time-outs that users can set. |
| | Icon double-click | Secure Immediately: Double-clicking the Secure Station icon secures the workstation. Show Display Options: Double-clicking displays the Secure Station Options dialog. |

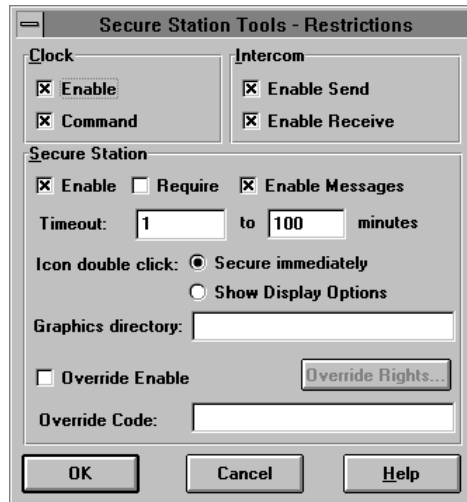
Continued...

| Module | Options | Results |
|--|--------------------|---|
| | Graphics directory | Limit user screen saver choices to the .BMP and .WMF files in this network directory. If blank, user can select from a standard McAfee list, plus all the .BMP and .WMF files in his Windows directory. |
| Note: See the “Secure Station Administrator Override” section below for more details on the following three fields. | | |
| Secure Station Tools | Override Enable | Checked: The administrator can override workstation security using the Override Code. Unchecked: Only the user logged on at this workstation can unsecure it. |
| | Override Rights | Displays the Override Rights dialog box, in which you select the network user ID’s permitted to use the override code. |
| | Override Code | Entry code allowing specified network ID’s to unsecure a secured workstation. The code is not case sensitive; it may be up to 128 characters long. |



To set restrictions on security modules

1. Choose Restrictions from the Options menu.



2. To enable the Clock, Command, Intercom Send, Intercom Receive, and Secure features, check the corresponding box.

A check in the box indicates the feature is active. You may select one or more of the five features.

3. Additionally, in the Secure Station group box you may:
 - Check the Require box to enforce the use of Secure Station. If you require the use of Secure Station, users cannot close Secure Station Tools, not even from the Task List.
 - Enter the Time-out limits within which users can set the time-out range for Secure Station Tools. Setting equal time-out limits creates a fixed time-out value.
 - Choose the radio button indicating the action performed when users double click on the icon (secure now or display options).
 - Limit user choices for Secure Station screen savers. If you enter a network directory here, users can choose only the bitmap (.BMP) files or Windows metafiles (.WMF) from that directory. If you leave this box blank, users can choose any .BMP or .WMF file in their Windows directory, as well as several graphics.
 - Enable the administrative override feature for Secure Station. See the “Secure Station Administrator Override” section below for more details.
4. Choose OK.

For details on using the Secure Station Tools modules, see Chapter 5, “Secure Station Tools.”

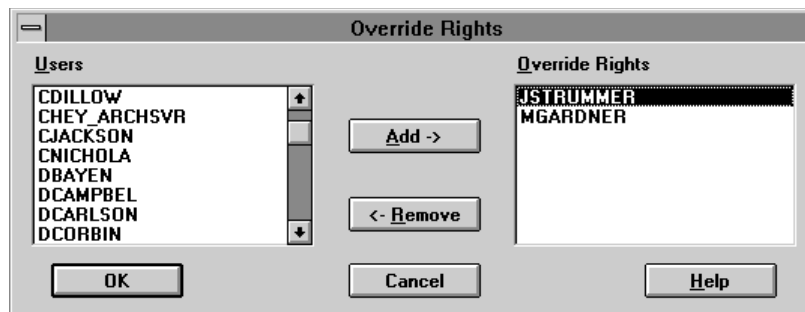
Secure Station Administrator Override

Occasionally, you may need access to a secured workstation, say to perform some maintenance, but the user is away. Even you, the network administrator, cannot get in if you don't know the user's password. So Desktop Administration includes an administrative override feature for Secure Station. If enabled, this feature allows network management personnel to gain access to any secured workstation on the network. To maintain a high level of security while still allowing administrator override, only the user ID's that you specify can use the feature, and those users will have to enter their network password.



To set up the override feature

1. In the Network Security - Restrictions dialog box, check Override Enable on.
2. Enter an override code. The override code applies to all workstations that read this WWEXT.WWR file. There is only one override code; you do not set different codes for each individual administrator.
3. Choose the Override Rights button to display the dialog box of the same name.



4. The Users list box shows all users on your primary server. Highlight a user and choose Add, or double-click a user to add them. The Override Rights list box shows the network ID's who will be able to override workstation security. No other network ID's will be accepted, even if they enter the override code.

The first time you display this dialog box, your user ID is added automatically.

5. Choose OK in the Override Rights dialog box.
6. Choose OK in the Secure Station Tools - Restrictions dialog box.
7. Save the .WWR file.

Now you can access a secured workstation by following these steps:

1. When the workstation is secured, move the mouse or press any key to get the Secure Station Password dialog box.
2. Type the Override Code in the Enter Password edit box, instead of the user's password.

If the override codes match, Secure Station displays the Password Override dialog box.



3. Select a server, enter your network user ID and network password. Only ID's that were selected in the Override Rights dialog are accepted. You may leave the user a brief message.
4. Choose OK.

The workstation unsecures.

If you left a message, the user receives it when she returns and unsecures her workstation. Even if you did not leave a message of your own, the user receives a message that you accessed the workstation. Also, if anyone tried to use the override feature but was unsuccessful, Secure Station leaves a message to that effect.

Exiting Desktop Administration

When you are ready to exit Desktop Administration, choose Exit from the File menu. If you have not saved your changes during the session, a message box requests that you save them. Choosing Yes in this box saves the changes in the current .WWR file and closes the program. Choosing No disregards any changes you may have made and exits.

If you have run the Administration program from Applications Manager, selecting Exit only closes the Administration program.

