

Chapter 4

Configuring On Guard

This chapter describes how to configure On Guard. The On Guard Installer program automatically creates one administrator and one startup user account. That is the typical configuration used by most On Guard sites. This chapter provides information for configuring On Guard to meet your security needs.

◇ Note On Guard's default configuration offers protection that suits most laboratory situations. When using the default protection, no additional configuration is required.

Entering the Configure application

There are two ways to enter the On Guard configuration application.

1. Select the Configure command from On Guard's Finder Menu. If the menu is not visible in the menubar, then hold down the option key before clicking in the menubar. If the menu still does not appear, then either the Finder Menu is disabled for the current user, or On Guard is turned off.

Figure 9. Selecting the Configure command.

2. At any time, you can launch the On Guard configuration application, which is found in your System Folder under System 6, or in your Control Panels folder in your System Folder under System 7. Figure 10 below shows the On Guard application. On Guard does not need to be turned on for you to launch the configuration application. You can also launch the On Guard application from the installation floppy disk.

Figure 10. On Guard Configuration Application.

When you launch the configuration application, On Guard asks for a name and password to ensure that only administrators perform the configuration tasks. This is shown below in Figure 11. The password is encrypted as you type so that it cannot be read by passers-by.

Figure 11. Administrator entering password to configure users.

◇ Note The default name for the administrator account is ‘Administrator’, and the default password is ‘admin’. You should change the password for the Administrator account as soon as possible. Failing to change the password from its default value could allow unauthorized users to modify or destroy important information on your Macintosh.

Quitting the Configure application

Select the Quit command from the File Menu to exit the Configure application.

Configure application menus

The On Guard Configure application offers three menus for performing configuration: File, Edit, and Panels. The File menu items open and save On Guard configurations, and quit the configuration mode. The Edit menu items cut, copy, and paste items, and restore the configuration options of the currently displayed panel to the original factory settings. The Panels menu items provide quick access to the On Guard configuration panels that are described in further detail in the remainder of this chapter.

Configuration panels

You modify the settings using On Guard's configuration dialogs. Choose between configuring User Options or Station Options by clicking the desired dialog.

- User Options take effect after a user signs on. User Options include the user's name, password, and individual security settings. There are five User Options panels.
- Station Options take effect as soon as your Macintosh starts up. Station Options include the ability to lock disks, view and print usage reports, and to change the Extensions bypass key from the shift key to an administrator-defined key. There are three Station Options panels.

To move through the panels, click a panel's tab in the tab bar at the top of its window or select its name from the Panels menu.

Restoring Factory Default Settings

Use the Defaults command under the Edit menu to return all the settings in the current panel to the default settings. This is helpful when you want to restore the settings to a known state.

Enabling or Disabling On Guard

Click the On/Off button, shown in Figure 12, to enable or disable On Guard. When the button is in the on position, all of On Guard's security is enabled, and when in the off position, all of On Guard's security is disabled. You can still use the On Guard configuration application when On Guard is turned off.

It is often convenient to simultaneously disable On Guard on multiple computers to install new software or perform routine maintenance. To do this you would:

1. Click the On/Off button to the Off position to disable On Guard.
2. Select the Save Settings To Network command in the File menu. This would disable On Guard on all specified computers. For more information see the section titled "Maintaining On Guard on multiple computers".
3. Perform your installation or maintenance.
4. Click the On/Off button to the On position re-enable On Guard.

5. Select the Save Settings To Network command in the File menu to re-enable On Guard on the other computers.

Users

The Users panel shows a list of user accounts that are currently registered with On Guard. Using this panel you can add, duplicate, or delete user accounts, or select which user account to configure. You also specify whether the On Guard security is enabled or disabled.

Select an account by clicking its name in the list, shown in Figure 13.

Figure 13. The Users panel.

Changing an existing account

1. Select the user to configure from the list.
2. Click the tab bar of the configuration panel you wish to go to, or use the Next menu command to take you to the Account panel.

Adding new users

1. Press the button labeled New User. A dialog box appears that allows you to enter the new user's name and password.
2. Enter the new user's name and password. The new user will then be added to the list that is displayed in the Users to Configure panel. User names must be unique.
3. Choose or create a folder that will be assigned to that user, as shown in Figure 15. The best location for the user's folder is at the root level of the hard disk, on the Desktop, or in a folder containing other users' folders. If you do not want a new folder to be created for a user, then click the No Folder button.

Figure 15. Creating a user folder for the User account.

Duplicating users

1. Select the user or users to duplicate from the list.
2. Click the Duplicate User button. The names of the new users will be appended with a suffix to ensure that the user name is unique. All other preferences, including the user's password, will be identical to the original user's preferences.

Deleting users

1. Select the user or users to delete from the list.
2. Click the Delete User button. The users will be deleted from On Guard's information.

If a folder was present for that user, On Guard will ask you if you want to delete the folder. If you choose to do so, then the user's folder and all of its contents, including all files and folders within the folder, will be deleted.

Copying and Pasting Settings

1. Select the user whose settings you would like to copy. Only one user's settings can be copied at a time.
2. Click the Copy Settings button.
3. Select the user or users whose settings you would like to be changed.
4. Click the Paste Settings button.

Copying and pasting settings replaces all the User Options for the account, excluding the name of the account, and optionally the user's password and folder.

Account

The Account panel controls general information about the user account, including the name, password, and folder.

Figure 16. Settings for the Account panel.

The user name and password appear in editable text fields. The password is displayed as a series of encrypted characters so that passers-by cannot read it.

Changing the user name

1. Select the name field using the tab key or the mouse.
2. Type in the new user name followed by the return key.

Changing the password

1. Select the password field using the tab key or the mouse.
2. Type in the new password, followed by the return key. On Guard will ask you to retype the password so that it can verify that the password is saved correctly. The password is automatically encrypted so that it cannot be read by passers-by.

Assigning a folder to a user

If the Folder box is checked, the user is assigned the named folder. If the user does not have a folder, then the box is unchecked and the folder's name reads as "<none>", as shown in Figure 16.

To change the assigned folder:

1. Uncheck the Folder box. If it is already unchecked proceed directly to the next step.
2. Click the Folder box to make it checked.
3. Select a folder using the selection dialog On Guard presents to you. You either select an existing folder, or create and select a new folder using this dialog.

Assigning a specific folder to a user is convenient when the user needs to save large files that would not fit on a floppy disk, but you wish to stop the user from saving files to other folders on the hard disk.

Assigning administrator privileges

When the Is Administrator box, shown in Figure 16, is checked, then the user is an administrator and may configure all user accounts and have access to all files, folders, and disks on the computer. To safeguard your computers, only assign administrator privileges to persons with a need for unrestricted access to the computer.

Assigning a Startup User

When the Is Startup User box is checked, then this user becomes the active user when the Macintosh starts up.

Having a Startup User account is convenient in environments where users should not be required to type a name and password. Several people can use the same Startup User account, making On Guard easier to use and configure.

The Startup User cannot have a password, and there can be only one Startup User account per computer.

Security

The Security panel controls which items the user can launch, open, save, copy from, view, and eject. On Guard provides two levels of security. The tab bar at the top of this panel allows you to switch between broad categories of security options with the first six tabs, and detailed security options with the tab labeled Advanced. The Advanced security panel allows you to set the security options of each item on any disk connected to the Macintosh computer.

The Security panels, figures 18—23, allow you to configure how users interact

with disks, users' folders, the System Folder, control panels, and the Chooser.

Launch

Select the Launch tab to show where the user can launch applications.

Figure 18. Settings for the Launch security panel.

If a box is checked, the user is allowed to launch applications from that disk or folder. Unchecking the box prevents launching applications, control panels, or desk accessories from that disk or folder.

Disabling Control Panels

In the Launch panel, uncheck the Control Panels box to prevent the user from accessing the control panels. If this box is checked the user will be able to modify many of the characteristics of your computer, including the desktop pattern, date, time, Finder fonts, the viewing modes, etc.

We recommend you disable control panels except under rare circumstances. However, it is sometimes important to allow advanced users to access certain control panels. To give access to certain control panels, see "Allowing Access to

certain control panels” in the section on “Advanced Security” below.

Viruses are commonly spread by launching applications on floppy disks. By stopping the user from launching applications on floppy disks, On Guard prevents the use of unauthorized applications and helps to reduce the possibility of viral infection.

Open

Select the Open tab to show where the user may open files and folders.

Figure 19. Settings for the Open security panel.

If a box is checked, the user is allowed to open the item in the Finder and Open dialog. If a box is not checked, then the user cannot open the folder or items within that folder. In Figure 19 below, the user cannot open other users’ folders or the System Folder.

Save

Select the Save tab to show where the user can save information. If a box is checked, the user is allowed to save to files within that disk or folder. If a box is

not checked, then user cannot move, delete, reposition, or otherwise modify items within that disk or folder. If the box is not checked then the user also cannot use the Finder's Clean Up command to reposition items in the window for that disk or folder. In Figure 20 below, the user can only save to floppy disks and to the user's own folder.

Figure 20. Settings for the Save security panel.

Copy

Select the Copy tab to show from where the user can copy items.

Figure 21. Settings for the Copy security panel.

If a box is checked, the user is allowed to copy items from that disk or folder. Unchecking the box prevents unauthorized copying of your files and reduces software piracy. In Figure 21 above, the user can only copy from floppy disks and the user's own folder.

View

Select the View tab to show which items are visible to the user. If a box is checked, the user is allowed to view that disk or folder and the items within it. If the box is unchecked then the item is invisible to the user and will not appear in the Finder or within an Open or Save dialog. By making items invisible, On Guard provides a barrier against tampering.

Figure 22. Settings for the View security panel.

Turning off the view permission for other users' folders is a convenient way to ensure privacy among users and administrators. As an administrator, you can create a folder for your account, and On Guard will prevent that folder and its contents from being viewed by other users. This makes your folder a quick, safe place to keep documents and special-purpose applications.

In Figure 22 above, the user may view everything except other users' folders.

Eject

Select the Eject tab to show which disks the user can eject. If a box is checked, the user is allowed to eject that type of disk. If the box is unchecked then the item cannot be ejected by the user. In Figure 23 below, the user may eject floppy disks, network disks, and CD-ROM disks.

Figure 23. Settings for the Eject security panel.

Advanced Security

Select the Advanced tab to control which specific files and folders a user can launch, open, save, copy from, view, or eject. Unlike the more general security panels that provide control of general types of disks and folders, the Advanced Security panel provides complete control of each individual disk, folder, and file on your computer.

Setting security permissions

The Advanced panel is shown below in Figure 24. To the right of each item are up to six letters. These letters indicate the user's Eject, Launch, Open, Save, Copy from, and View permissions.

Click a letter to change the user's security permissions for that item. If the letter has a box around it, then the user can perform that operation on that item. If the letter is not boxed, the user cannot perform that operation.

Figure 24. Advanced Security settings for an Applications folder.

The settings for a folder extend to all items within that folder. For example, if you have a folder whose save permission is turned off, then the user cannot modify any item within that folder or its subfolders.

Moving to an item

You move to disks, folders, or files within the Advanced panel in a similar manner as within the Macintosh Open or Save dialogs. The list on the left side of the panel displays the items within the current folder. The current folder or disk is displayed in the popup menu above the list. Click the popup menu above the list to show the contents of folders higher in the hierarchy. Double-click any folder to move down into that folder. You can also use the Go To popup menu to go directly to specific folders such as the Desktop folder or the Control Panels folder.

Permission options

Permission options are the same as in the standard Security panel.

Launch

If boxed, the user may launch applications, desk accessories, and control panels in that location. If not boxed, the user cannot launch items in that location.

Open

If boxed, the user has permission to open that item in the Finder or in the Open dialogs.

Save

If boxed, the user may make changes to the item. If a file is not boxed then the user cannot delete or edit that file.

If a

folder is not boxed then the user cannot create, save, duplicate, delete, or reposition items within that

folder.

Copy from

If boxed, the user may copy items from that location. If not boxed, the user cannot copy any files or folders from that

location. This prevents unauthorized copying of your

files

and help prevent software piracy.

View

If boxed, the user may view items in that location. If not boxed, the item will be invisible in the Finder and within any Open or Save dialog. By removing View permission, you can keep records and special-purpose applications away

from users.

Eject

If boxed, the user may eject the disk. If not boxed, the user cannot eject the disk. This box only appears for disks.

Allowing access to certain control panels

1. While in the security panel, click the Launch tab to go to the Launch panel. Uncheck the Control Panels box to disable launching all control panels.
2. Click the Advanced tab to get to the Advanced Security Panel, then move into the Control Panels Folder. You can use the Go To popup menu to go directly to the Control Panels folder.
3. Turn on Launch permission for all the control panels you want the user to access. To turn on permission for an item, click the letters for that item until the letter is boxed. In Figure 25, only the Monitors control panel is available to the user.

Figure 25. Enabling the Monitors Control Panel.

Creating Drop Folders

Using On Guard, you can create a special kind of folder called a Drop Folder. Drop Folders are useful when you want a user to be able to leave information in a folder for you or another user without seeing what other information is already in that folder.

To create a Drop Folder:

1. Move to the folder in the Advanced Security panel.
2. Turn on Save, and View permission for the folder.
3. Turn off Open, Launch, and Copy from permission for the folder.

Finder

The Finder panel allows you to specify how the user interacts with menus in the Finder, including On Guard's Finder Menu.

Displaying On Guard's Finder Menu

The radio buttons specify whether On Guard displays its Finder Menu, the menu is hidden, or there is no menu for the current user. To access the menu when it is hidden, you must hold down any of the command, shift, option, or control keys before clicking in the menubar.

Figure 26. Settings for the Finder panel.

When there is no menu for the current user, the Sign Off and Configure commands are not accessible via the Finder Menu. However, you can still perform these actions without using the Finder Menu. To sign off, you can use the sign off key defined in the Sign On panel. See the section on the Sign On Panel in the Station Options section of this chapter for details on how to set the sign off key. To configure, you can launch the Configuration Application directly. See the beginning of this chapter for information on how to launch the Configuration Application.

Enabling the Sharing command (System 7 only)

Check the Enable Sharing Command box to allow the user to accessing the Sharing menu item in the Finder. This command is used to mark items as sharable for File Sharing. Ordinarily, you will not want users to modify the Sharing settings for items.

Put away ejected floppies

Check the Put away ejected floppies box to automatically remove ghost icons when a disk is ejected. When floppy disks are ejected using the Eject command, a ghost icon for the floppy disk would ordinarily remain on the Macintosh desktop.

When a ghost icon remains on the desktop and the original floppy disk is not available (for example, if the user who ejected the disk is no longer there), the

Finder will repeatedly ask for the floppy disk that was ejected. Pressing command-period will stop the Finder from asking for the floppy disk, but many users do not know this. Automatically putting away the ejected floppy disk will prevent the ghost icon from remaining on the desktop and solve this problem.

System

The System panel allows you to disable the following advanced Macintosh features.

Enabling screen capture

Check the Enable Screen Capture Command box to allow the user to use the Command-Shift-3 key sequence to perform screen captures. If this box is checked the user can use the screen capture command until the disk becomes full.

Enabling Force-Quit (System 7 only)

Check the Enable Force-Quit Command box to allow the user to use the Command-Option-Esc key sequence to quit applications or the Finder. Using the Force-Quit command to quit applications or the Finder sometimes causes your computer to crash.

Enabling the Interrupt switch

Check the Enable Interrupt Switch box to allow the user to activate the system debugger. The interrupt switch is available on most Macintosh models and is used to display the system debugger window.

Figure 27. Settings for the System panel.

Station Options

The Station Options dialog allows you to set station-wide options. These options take effect when the computer starts and remain in effect for every user. You access the Station Options panels by clicking the Station Options dialog, or by going to the Panels menu and choosing the command for one of the Station panels.

Startup

The Startup panel allows you to assign an extensions bypass key and lock disks.

Specifying the Extension Bypass Key

The Extensions Bypass Key box overrides the Shift key at system startup to disable extensions. Apple programmed an extension bypass key into System 7 as a safety feature. Pressing the extension bypass key stops all extensions and control panels from loading, including On Guard.

Figure 28. Startup Options panel.

You can provide a key combination to override the extension bypass key. On Guard allows you to choose any combination of the command, shift, option, and control keys, along with one key from the normal keyboard, as the extension bypass key. For example, you can specify that the command, option, and S keys be held down simultaneously, as shown in Figure 28, to disable extensions from loading. Hold down the delete key in this text box to totally disable the extensions bypass key.

◇ Note Under System 6, the extension bypass key specified in the Startup panel only prevents On Guard from loading.

Disks Locked

To prevent users from modifying hard disks when your Macintosh is booted with a System floppy disk, check the lock to the left of the desired disk until the lock icon appears to be locked. You can specify which disks are to be locked by a broad category of disks, such as Startup Disks, or by the specific disk that is currently connected to your computer.

When you boot from another System disk or when extensions are disabled, you must launch an unlocking application, then enter a valid administrator's name and password to unlock the disks before you can use them. When disks are locked you cannot access any existing files.

Figure 29. Launch this application to unlock the hard disks.

To unlock the disks, launch the application shown below in Figure 29 and enter an administrator's name and password.

After the disk is unlocked, it is unprotected until the next time your computer starts up with On Guard installed.

Sign On

The Sign On panel allows you show a menu of user names when signing on and assign a key that will sign a user off.

Show user menu when signing on

When the box is checked, On Guard will show a popup menu of user names when a user is signing on. A menu of user names is convenient in environments where users can be given a list of names to choose from. If you have had problems with users attempting to break in to other users' accounts, we recommend disabling this feature because it gives the user a starting point for breaking in.

Click the Show Administrators in Menu box to include administrators' names in the popup. To reduce the possibility that a user could break in using an administrator's name and password, do not check this box.

Figure 30. Sign On Options panel.

Assigning a Sign Off Key

The key combination defined in the text box will sign the current user off when the Finder is the current application. Because this is a Station Option, all users on a particular computer will use the same Sign Off Key. If the Finder menu is turned off for a user in the Finder panel, this is the only way to sign off.

Reports

The Reports panel allows you to display information gathered by On Guard about how the Macintosh has been used.

On Guard constantly monitors all activities. The report displays information only about the computer that On Guard is installed on. Click the checkbox for the type of information you want to see in the report.

Figure 31. Reports panel.

On Guard allows you to display the following information in a report.

- **Users.** Use the Users popup to specify the user or groups of users whose information you want to display.
- **Size.** Use the Size popup to specify the maximum hard disk space that the On Guard report will occupy. If None is selected, no report is maintained.
- **Startup & Shutdown.** Check the Startup & Shutdown box to display information about the computer's startup and shutdown procedures . The report includes the time the computer is started up and shut down, the consecutive hours the computer was turned on, and whether the computer was shutdown properly.
- **Signing On & Off.** Check the Signing On & Off box to display information about when users signed on and off the computer. This report includes the time of day the users signed on and off, the consecutive hours the user was signed on, and how the user was signed off.
- **Idle.** Check the idle box to display information about when the computer was idle. The popup menu lets you specify the minimum time the computer must remain idle before an item is placed in the report. Each idle period greater than the minimum time will be displayed as one line in the report. For example, if the popup is set to 15 minutes, and the computer was idle for 45 minutes, one item reporting that the computer was idle for 45 minutes would be displayed in the report.
- **Opening.** Check the Opening box to display information about which files were opened.
- **Saving.** Check the Saving box to display information about which files were saved.
- **Copying.** Check the Copying box to display information about which files were copied. Both the files that were copied and their destination will be displayed.
- **Launching.** Check the Launching box to display information about

which applications, control panels, and desk accessories were launched.

- **Violations.** Check the Violations box to display information about any security violations detected by On Guard. These include incorrect user name and password entry, file saving, copying, opening, and application launching that were denied by On Guard, and any other action that On Guard prevented from occurring.