CONTENTS

SECTIONS

Gatekeeper's controls and displays are separated into six sections each of which is briefly described below. The list of available sections always appears at the top of Gatekeeper's window, and it may be necessary to use the scroll bar to see all the items in the list.

Clicking once on a line in the list opens the appropriate section of Gatekeeper. If you prefer to use the keyboard, you can hit the tab key to move to the next item in the list and shift + tab to move to the previous item in the list.

1 – GENERAL

The General section is always the first section visible when Gatekeeper is opened. It will tell you the version number of Gatekeeper and may, in future versions, bring other information to your attention as necessary.

2 – HELP

This is Gatekeeper's help section. It provides a quick description of the controls and displays in all of Gatekeeper's sections. For an introduction to Gatekeeper refer to the Gatekeeper Introduction file which should have been included with this copy of Gatekeeper.

You can move up and down in the help text using the scroll bar or the page up and page down

keys on some keyboards. The home and end keys on those keyboards can be used to move to the top and bottom of the help text, respectively.

Text from the help section may be selected using the mouse and copied to the Clipboard so that it can be pasted into other applications. This would allow you, for instance, to paste the text into a word processor and print it out.

3 – ON/OFF

The ON/OFF feature allows you to turn Gatekeeper off for a user-specified length of time. This is useful when you're performing tasks that Gatekeeper would otherwise interfere with. The most common examples of such tasks are running "installer" programs which load software of some kind onto your system. Common examples of software loaded using these programs include Microsoft Word and Excel, and Aldus PageMaker.

The maximum length of time Gatekeeper can be off is displayed next to the "Time Limit:" label in this section. To change the limit, just click on the time limit numbers and edit them the same way you would edit the time setting in the General control panel or the Alarm Clock desk accessory. When you're finished editing the time limit, hit the return key.

When Gatekeeper is off, the value displayed next to the "Time Remaining:" label in this section will tell you how much time remains before Gatekeeper automatically turns itself on again. When Gatekeeper is on, the value displayed3ys zero.

Remember that Gatekeeper will not provide protection against viruses while it is off.

4 – SETTINGS

The Settings section allows you to define some of the basic ways in which Gatekeeper operates.

When a Privilege Violation Occurs

Two radio buttons in this area let you tell Gatekeeper what to do about suspicious operations it encounters. When the "Stop the Operation (Notify & Veto)" radio button is selected, Gatekeeper will stop any suspicious activities it observes. On the other hand, if the "Permit the Operation (Notify Only)" radio button is selected, Gatekeeper will not interfere at all with suspicious operations; it will merely tell you the operations have occurred. It's then up to you what you do about them.

When an Important Event Occurs

Two check boxes in this area let you tell Gatekeeper what it should do when it needs to get your attention. Typically, Gatekeeper only needs to get your attention when it observes privilege violations or other similarly unusual events. The “Display an Alert” check box tells Gatekeeper, when it is used with System 6.0 or later, to display an alert describing the event that occurred. The “Record it in the Log File” check box tells Gatekeeper to record a short description of the event in the Gatekeeper Log file for later review. These two options may be used in any combination you find convenient; in practice, however, it’s best to keep both options checked.

During Startup

Two check boxes in this area let you tell Gatekeeper how to behave when your Mac starts-up. If the “Show the Gatekeeper Icon” check box is checked, Gatekeeper’s icon will be displayed somewhere along the bottom of your Mac’s display during startup. Showing the icon in this fashion is merely a convenient way of indicating that Gatekeeper is installed on your Macintosh. In addition, if Gatekeeper cannot install itself for some reason, the icon will be drawn with a large red X over it to warn you that something went wrong.

The other check box in this area, labeled “Display a Mode Warning Alert”, allows you to tell Gatekeeper whether or not it should display a “warning” alert after startup to remind you of the mode in which it is operating. Gatekeeper can operate in either Notify Only or Notify & Veto mode. (A quick explanation of these modes can be found at the beginning of the Settings section in this help display.) By default, Gatekeeper displays a warning alert after startup when it is in Notify Only mode (since it doesn’t protect against viruses in that mode), but does not display a warning alert when in Notify & Veto mode (since that is the mode in which Gatekeeper normally operates). The “Display a Mode Warning Alert” check box, however, allows you to change this behavior to suit your own needs.

5 – LOG

This section allows you to view the contents of Gatekeeper’s log file, if the “Record it in the Log File” option is checked in the Settings section. The log file is a file in which Gatekeeper records all the important events it observes for your later review.

Selecting a line in the log file display and clicking on the Get Info button will bring up an alert which explains the event recorded on that line of the log file. Double-clicking on a line, or clicking on a line and hitting the return or enter keys has the same effect.

For the convenience of users with appropriately equipped keyboards, the following keyboard shortcuts are available. To select the next line above or below the currently selected line use the up-arrow and down-arrow cursor keys. To move up or down through the log quickly, use the page up and page down keys. To instantly move to the top or bottom of the log, use the home and end keys, respectively.

Normally, the log will contain only “Startup” and “Shutdown” messages, which tell you when

your Macintosh has been started or shutdown in Gatekeeper's presence. These messages are totally routine, and are recorded only to help you determine when your Mac has been used and whether it may have been used without Gatekeeper, thereby leaving it unprotected against possible virus attacks.

The really important entries in the log file are displayed in bold, red type to get your attention. These entries normally describe attempts by programs to exceed the privileges they have been granted. These entries may tell you one of two things: (1) some program needs additional privileges in order to operate correctly, or (2) a virus is attempting to spread on your Macintosh and is being stopped by Gatekeeper. If you're not sure which is which, try running Disinfectant 3.2, or later, to check for the involvement of known viruses. For additional information and helpful advice, you may want to refer to the Log section of the Gatekeeper Introduction document.

However, if you are confident that an entry in the log file merely indicates that a program needs additional privileges in order to operate correctly, you can grant that privilege by selecting that entry and clicking on the Get Info button. This will bring up an alert describing the entry. That alert will include a large button labeled Grant Privilege; clicking on that button will give the guilty program the privilege described in that entry. After using the Grant Privilege button, you can, if you wish, switch to the Privileges section where you'll find that the guilty program has been automatically selected in the privilege list, in case you need to make adjustments.

6 – PRIVILEGES

The list that appears in this area is the list of applications that have been granted privileges of some kind. To the right of the list are four buttons: "Add", "New", "Edit" and "Clear". "Add" permits you to add an item to the list using the normal "Open" dialog box. You can compel Gatekeeper to display files regardless of their types by holding down the option key when clicking on the "Add" button. "New" gives you the option of typing in the name of an item to be added to the list; this is a convenient alternative to the "Add" button, and just about the only way to give privileges to desk accessories. "Edit" lets you change the name of the currently selected item in the list. "Clear" allows you to delete the currently selected item from the list.

For a sensible discussion of what the privilege check boxes for an item mean, see the "Gatekeeper in Principle" section of the Gatekeeper Introduction document.

For the convenience of users with appropriately equipped keyboards, the following keyboard shortcuts are available. To select the next item above or below the currently selected item use the up-arrow and down-arrow cursor keys. To move up or down through the list quickly, use the page up and page down keys. To instantly move to the top or bottom of the list, use the home and end keys, respectively.

To select an item by name, type in the first several letters of its name; the list will be scrolled to the item that comes closest to matching the letters you've typed.

To delete an item from the list use the backspace, delete or clear keys. To edit the currently selected item, double-click on it, or hit the return or enter keys.

COPYRIGHT NOTICE

Gatekeeper ©1988-1993
Gatekeeper Aid ©1990-1993
by Chris Johnson.

All Rights Reserved.

Gatekeeper and Gatekeeper Aid are free for non commercial public distribution. This software may not be sold or distributed for profit, or included with other software which is sold or distributed for profit, without the permission of the author. (CD-ROM publishers are not now, nor have they ever been, an exception to this rule.)

To put it simply, I don't make any money from this software, so nobody else should either.

While there is no charge for Gatekeeper, I do ask that if you use this product, you send me a picture postcard from your home town (or from wherever you happen to be at the time). If that's too much to ask, find a comparable product with more reasonable terms....

POSTCARDS, BUG REPORTS, ETC.

I can be reached with questions, suggestions, bug reports (be sure to note the version number of Gatekeeper and/or Gatekeeper Aid that you were using), etc. at…

Internet:
chrisj@emx.cc.utexas.edu

UUCP:
husc6|uunet!cs.utexas.edu!ut-emx!chrisj

AppleLink:
chrisj@emx.cc.utexas.edu@internet#

CompuServe:
>INTERNET:chrisj@emx.cc.utexas.edu

MCI Mail:
Command: Create
To: Chris Johnson (EMS)

EMS: Internet
MBX: chrisj@emx.cc.utexas.edu

US Mail:

Chris Johnson
Gatekeeper
4505-B Avenue H
Austin, TX 78751

Turnaround time on email messages is usually under 48 hours, if I'm not drowning in mail at the time. If I am drowning in mail at the time (an increasingly common situation in the last few years), it'll definitely take longer to get back to you. Turnaround time on US Mail is approaching five years in many cases. So, if you have the choice, send email. If you must use US Mail, including a self addressed stamped envelope just might help to speed up the process.

...and please send a postcard. (See the Copyright Notice above.)

(Of course, if you use this product and happen to work for Apple Computer, feel free to convince Apple to contribute a fast Macintosh computer system of some sort as a way of finally showing some support for this development effort.)

See the Gatekeeper Introduction document for additional details on all this stuff.

FINDING THE LATEST VERSION

There are several good ways to find the latest version of Gatekeeper:

1. People with FTP access to the Internet can retrieve the latest version via anonymous FTP to the microlib/mac/virus directory of microlib.cc.utexas.edu. Of course, there are many other good archive sites which should also have current versions at any given time, but I upload new releases directly into microlib as soon as they're ready, so I can guarantee that it's up to date.

2. If you can send me email, I can usually email the latest version back to you. Be sure to let me know what version you are currently using. There can be problems, however. Some services like AppleLink and CompuServe limit the length of messages their users can receive to something in the neighborhood of 32K. This means that I'd have to split Gatekeeper into more than 12 parts in order to send it via email (and the recipient would subsequently have to reassemble all those parts). This is very time consuming, so unless your mail system will accept messages close to 100K in length, it's probably not a good idea to try to get Gatekeeper via email. Remember to tell me the maximum message length your system will accept.

3. U.S. Mail is also an option. Send a diskette along with a self-addressed, stamped envelope

(SASE) to the address below. Unlike correspondence, I am able to periodically catch-up on all the outstanding update requests, so you really will get your disk back eventually. Unfortunately, disks sent without a SASE (or a reasonable facsimile), legible return address, correct postage, etc. can't be returned. I will occasionally replace a bad or damaged diskette out of my own pocket, but don't count on it. In other words, don't send me that old diskette that you found under the refrigerator last spring. I probably won't be able to format it successfully, and you'll always wonder why you didn't get your disk back.

Anyway, the address to send those disks to is:

Chris Johnson
Gatekeeper Update from 1.2.8
4505-B Avenue H
Austin, TX 78751
USA

The "Gatekeeper Update…" line is important, so be sure to include it. Note that the "from 1.2.8" part tells me what version you are currently using so that I won't make the mistake of sending you a version which you already have.

…AND THANKS FOR ALL THE FISH

Many thanks to all the Gatekeeper testers. Without their help and patience Gatekeeper couldn't have been made even remotely as reliable and trouble-free as it is.

Scott R. Anderson
Dale M. Arends
Brian Aslakson
Steve Baumgarten
David A. Belsley
Sunil Bhatla
Thomas R. Blake
James Blieden
Jonathan Brecher
Daniel Buchan
Rick Cardona
Ian Chai
Philippe Chatalic
Brian L. Donnell
Jon Duke
Jim Elliott
Bill Engels
Zbigniew Fiedorowicz
Charette Frederick

Brian Gaines
Peter Galko
David A. Grayson
Ben Goren
Marcus Harvey
Jay Hirsh
Steve Holden
Kirk Holub
Dan Hugo
John Im
David Inman
William G. Innanen
Andrew E. Johnson
Vahe Kassardjian
Kendrick Killian
Edgar Knapp
Dick Kriss
Dave Lee
Masato Ogawa
Doc O'Leary
John Owens
John F. Pane
Peter John Roberts
Clay C. Ross
Nick Rothwell
Robert Rubinoff
Howard Shubs
Larry Simmons
Robert Stewart
Michael Stovsky
Jochen Teufel
Werner Uhrig
Johan van Zanten
Mike Weasner
Jerry Wilcox
Thomas Willett
Ed Wright
Marvin Yount
David R. Zinkin
Sam Zschokke

I would also like to thank all the people around the world who have sent me problem reports at one time or another. Unfortunately, there's just no testing ground quite like the real world. There are too many people to list (and, in fact, too many to keep track of), but they know who they are. Thanks to all.

Thanks to Ken McLeod for his translation of the original ShowINIT code into THINK C. There's only a few lines of his code left in Gatekeeper's ShowINIT implementation, but I'm glad I had that code from which to work. Patrick C. Beard's code was also helpful, but none of it survives into this implementation.

Gatekeeper and Gatekeeper Aid were built with version 5.0.4 of THINK C.

DISCLAIMER

My employer is in no way responsible for – or even remotely involved with – the Gatekeeper project.