

# GateKeeper

Release Notes for version 1.1.1 of 26-Jun-89 by Chris Johnson

## Introduction to GateKeeper

The file "Introduction to GateKeeper" is a MacWrite document which offers a brief introduction to the principle and practice of GateKeeper. If you're already familiar with GateKeeper it won't be anything new to you. If, on the other hand, you've never dealt with GateKeeper before, read it before proceeding – GateKeeper's not complicated, but it's not simple either and the introduction should help make it all more sensible.

The document will look best if you have the New Century Schoolbook and Times fonts.

## Installing GateKeeper

Installing GateKeeper is straightforward, but before doing so take a minute to make a backup copy. If you want to give anyone else a copy of GateKeeper give them a copy from your backup. GateKeeper is released preconfigured in "Notify Only" mode for safety in installation and it comes with a privilege list containing many of the most commonly required privileges. Along with GateKeeper there should also be a "READ ME" file, these release notes and the "Introduction to GateKeeper" document. Every copy of GateKeeper distributed should be configured in this manner and should include these documents.

If you haven't dealt with GateKeeper before this would also be a good time to read the introduction document and finish reading these release notes.

To install GateKeeper simply drag it into your System Folder and restart your Macintosh. By default, GateKeeper will create a file named "GateKeeper Log" in the System Folder. You can be sure that GateKeeper is installed if its icon appears in the Control Panel.

## Privileges

GateKeeper 1.1.1 comes preconfigured with approximately 40 of the most commonly required privileges in order to make installation of this new version simpler and faster. Remember, however, to go through the privilege list and delete the entries for any programs that you don't use.

While you're at it think about how often you use the programs in the privilege list. If you don't use programs like Font/DA Mover (which only needs privileges when installing/removing desk accessories), ResEdit or Disinfectant routinely, they shouldn't be given privileges. Just place GateKeeper in Override mode when you do use these programs.

The key thing to remember is that privileges allow programs to carry out actions that appear virus-like to GateKeeper. Privileges will also let viruses carry out virus-like actions, so give privileges where you need them – that's what they're for, after all – but don't give them unnecessarily.

Should you need it, the complete list of default privileges is reproduced at the end of this document. If you find the list of privileges incomplete or inaccurate, please let me know. I can be contacted at any of the addresses listed in GateKeeper's on-line help.

## A Known Bug

GateKeeper will cause a System Error during "switch-launches." This has been true of all versions of GateKeeper, but will – if I can get the information I need – be fixed in a future release. My apologies for any inconvenience this bug may cause (I'm not happy about it either.)

A "switch-launch" is defined by Apple to occur in the following situations:

- When you hold the Option key while you open an application that's on another startup disk.
- When you hold down the Option and Apple (Command) keys while you double-click the Finder icon on the disk you want to switch to.

Since these are not operations you're likely to carry out frequently or unwittingly, this bug may never cause you any problems, but I thought you ought to know about it.

Of course, if you're using MultiFinder, switch launches simply cannot occur, so you'll never have to worry about this.

### **Changes Since Version 1.1**

A serious bug in the version 1.1 code responsible for manipulating the privilege list has been fixed. At the same time, new features have been introduced to extend the flexibility of the security system.

GateKeeper continues to prove itself effective against all known viruses. The list currently includes Scores, nVIR, Hpat, INIT 29, ANTI, AIDS and MEV#.

Version 1.1.1 adds explicit awareness of the two new nVIR clones, AIDS and MEV#, in order to prevent false alarms from virus scanners. Nonetheless, even without this awareness, GateKeeper was fully effective against those viruses.

### **OLD PROBLEMS**

The primary problem with 1.1 was a bug that caused either temporary or permanent corruption of the privilege list. Although it didn't cause everyone trouble, a very few people found GateKeeper completely dysfunctional as a result. Others found GateKeeper acting as though it'd forgotten some or all of its privileges, no matter how the privilege list read in the Control Panel. Still others simply found the privilege list trashed or empty on rare occasions, but were spared the more serious effects mentioned above.

### **NEW FEATURES**

Although version 1.1.1 is primarily a maintenance release intended to correct bugs rather than add new functionality, a few new features have found their way in as a result of users' problem reports and suggestions.

#### **THE "ADD..." DIALOG BECOMES MORE TOLERANT**

In past versions the dialog box that appeared when the "Add..." button was clicked only displayed files of certain types. Although this was normally sufficient, some people, particularly MPW users, discovered that they couldn't grant privileges to all the files that needed them.

Version 1.1 improved on this by allowing the user to hold down the Option key when clicking on the "Add..." button in order to see a complete list of files. Although this fixed the problem in principle, it didn't do such a great job in practice - many users never noticed the Option key trick in the on-line help.

Version 1.1.1, by default, displays almost every file on disk that has a resource fork. This should completely eliminate the problem. (Of course, the Option key trick is still there if you should ever find a need for it.)

#### **NAMES IN THE PRIVILEGE LIST BECOME EDITABLE**

In the past, if you needed to alter a name in the privilege list, you had to clear it and then add it all over again. Now you can simply select it in the list and click on the new "Edit..." button. Of course, if you'd rather take the easy way out, you can just double-click on the item.

#### MORE FLEXIBLE NAME MATCHING

Two extensions have been made to the portion of the GateKeeper security system responsible for looking-up names in the privilege list. Both work to make GateKeeper more tolerant of strange circumstances and simple file name variations.

#### MATCH BEGINNINGS

If this option is turned on, only the beginning of a program's name is required to match an entry in the privilege list, anything left-over is ignored.

In particular, this lets you build a more generalized privilege list. For instance, you can simply create an entry in the privilege list for "Font/DA Mover" without worrying about whether users' applications will actually be named "Font/DA Mover 3.8" or just "Font/DA Mover".

#### IGNORE CASE

If this option is turned on, no distinction is made between letters of different case, so "font/da mover" would be considered to match "Font/DA Mover", and "link" will be considered to match "Link". MPW users, take heed.

#### INTERNAL ERRORS

Internal Errors can now be avoided by granting all three File privileges to the applications that cause these errors.

This will be of particular use to users of old versions of MacWrite and pre-1.1 versions of MacDraw.

#### SetResAttrs() MONITOR ALTERED

The SetResAttrs() routine is a part of the Toolbox's Resource Manager. It is often used (or misused, depending on how you look at it) in the process of loading INITs.

In the past, GateKeeper has been very strict about restricting the use of this Toolbox routine. This resulted in many INITs and a few applications (most notably Microsoft Excel) needing privileges in order to carry out what might be looked upon as rather trivial operations.

GateKeeper 1.1.1 is less strict about the use of this routine. This should help reduce the number of INITs and applications that require Resource privileges. MS Excel, for instance, no longer requires privileges (of course, it really shouldn't have done what it was doing with SetResAttrs() in the first place.)

#### AT STARTUP: ICON

You can now choose whether or not GateKeeper shows an icon at the bottom of your screen while your system starts-up.

In addition, a more literal adaptation of Paul Mercer's ShowINIT code is used in this version. This eliminates the conflicts between GateKeeper and INITs like Flex and Fontsie. As a result, there are no longer any INITs that are "fundamentally incompatible" with GateKeeper.

#### MATCH BEGINNINGS

The "Match Beginnings" option has been altered to ignore leading spaces (breaking and non-breaking) in both privilege list entries and actual file names.

## THE LOG FILE

The GateKeeper Log File is now locked when the Macintosh starts-up and is unlocked when it shuts-down. Because of this, many programs that would not normally understand how to open a busy file will be able to do so. In particular this means that the McSink desk accessory and Microsoft Word 4 can now open the log file.

Program Name	Res Privileges	File Privileges
Finder		Other
AppleLink		Other
BinHex		Other
Blitzmail		Other
Blitznotify	Self	
Clock Adjust	Self	
DA Handler		Other, Sys, Self
Demo Appmaker	Other	
Dimmer	Other	
Disinfectant	Other, Sys, Self	Other, Sys, Self
DiskFit		Other
DOctor		Other
FastBack		Other
FileSplitter		Other
FKKey Manager	Other, Sys	
FKKey/Sound Manager	Other, Sys	
Floppy Recover		Other
Font/DA Mover	Other, Sys	
Font/DA Utility	Other	
Full Impact		Other, Sys, Self
FX/FI Manager		Other
HD Tuneup		Other
HFS Backup		Other
HFS Recover		Other
HyperCard	Other	
init cdev		Other
InterMail	Self	
KSP	Self	
Layout	Sys	
Link	Other	Other
MacCompress	Other	Other
MacDraw II		Other, Sys, Self
MacTerminal		Other
MacTools		Other
MacWrite		Other, Sys, Self
MPW Shell	Other	Other
MutiInBox		Other, Sys, Self
Møre	Self	
NCSA Telnet		Other
PackIt		Other
RAM Disk	Self	
Red Ryder		Other
REdit	Other	Other
ResEdit	Other	Other
Resource Resolver	Other	
Rez	Other	
Scanner		Other
Spooler	Self	
Symantec Tools	Other	Other
THINK C	Other	Other
THINK Pascal	Other	Other
TOMvINIT	Sys	
Tops	Self	
Turbo Pascal	Other	Other
UnlockCode	Other	
Unstuffit		Other
Versaterm		Other
VideoWorks	Self	