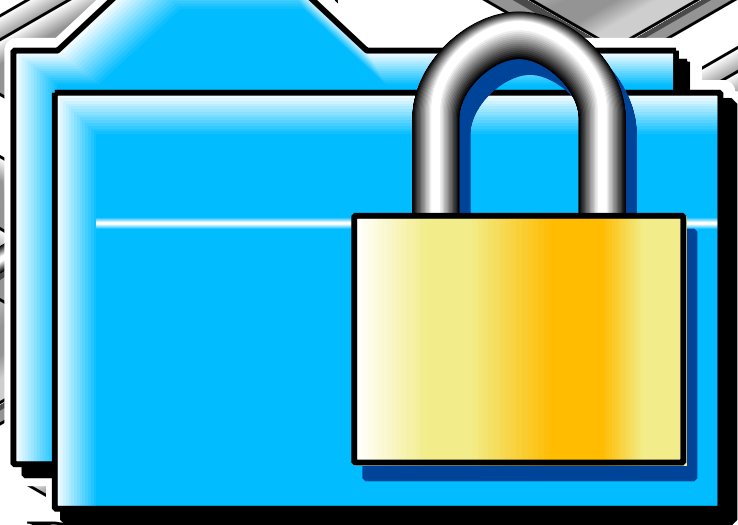


Desktop protection for Acorn computers
running the Universal !Boot Sequence



Desk
Lock

© 3QD Developments Ltd 2026

iSV
Products

3QD
DEVELOPMENTS LTD

APDL

DeskLock

Copyright © 3QD Developments Ltd 2026
All rights reserved.

No part of this product may be reproduced in whole or part by any means without written permission of the publisher. Unauthorised hiring, renting, lending, public performance or broadcasting of this product or its parts is prohibited.

While every care is taken, the publisher cannot be held responsible for any errors in this product, or for loss of data or consequential effects from the use of this package.

Software and Documentation supplied by
APDL
a part of
3QD Developments Ltd
Single User version downloaded from the free of charge software section of
www.riscos.com

Please note that any free of charge downloads from RISCOS.com are supplied without any technical support package as per the licence agreement.

This document last edited on 29/09/26



If you have found this application and this manual useful please consider making a donation to help cover the costs of cataloguing, documenting, updating and hosting the APDL applications. Scanning the QR code will take you to our donations page.

Introduction to DeskLock

DeskLock is a security system for Acorn computers running RISC OS 3.1 or later and with a hard disk. DeskLock prevents users accessing chosen directories and apps without the correct password.

DeskLock consists of two main applications, DeskLock & DeskPass. DeskLock itself is designed to be running all the time on the computer and should be installed in the computers boot sequence. As well as protecting apps & directories DeskLock also disables the Break key, prevents files being copied without a password & disables the F12 escape route from the desktop.

DeskPass allows a system administrator to configure the DeskLock application by dragging in those directories and applications which will be password protected.

Also supplied is an installer application (DeskInstl) which will install DeskLock onto any RISC OS 3.1 or later machine with a correctly set Boot sequence. In order to get full use of DeskLock we recommend that any OS 3.1 computers have the Universal !Boot system installed (as used on RISC OS OS 3.5 or later).

We strongly recommend installing the Universal !Boot sequence on any RISC OS computer. You can download this free of charge from the FTP section of RISCOS.com.

DeskLock and Emulation

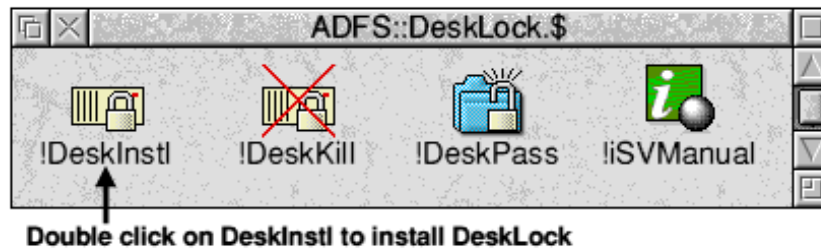
Installing DeskLock on an emulated system won't make that system secure in the same way as it does for a 'real' RISC OS computer. For example if DeskLock is installed into a copy of VirtualRPC in the **HostFS::HardDisc4.\$** drive it would be easy to just open the HardDisc4 folder in Windows, look inside !Boot and delete the DeskLock application. DeskLock will be more secure if the emulated system is booting from an ADFS harddisc image, as it's not as easy to edit these disc images, but it can be done.

DeskLock and RISC OS 5

Currently DeskLock isn't fully 32bit neutral and as such won't work correctly on RISC OS 5. We **very strongly urge you not to run DeskLock on a 32bit RISC OS 5 computer** because if things do go wrong you might have to re-install the !Boot sequence and possibly some applications. Once DeskLock has been fully converted to 32bit we will update this manual to reflect this.

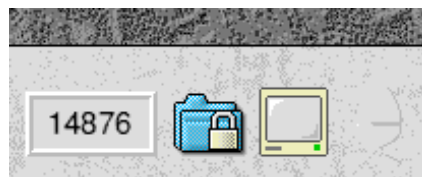
Installation

To install DeskLock on a computer simply double click on the !DeskInstl icon and DeskLock will be installed on the hard disk.



Provided that the computer has a correct Boot sequence DeskLock will now be loaded automatically every time the computer is turned on.

The DeskLock Icon will appear next to the task manager icon on the icon bar once the computer is re-booted.



Note that the Task Manager is now greyed out and cannot be used.

The computer is now protected. The next section will cover the use of DeskLock.

Using DeskLock

DeskLock will perform the following actions:

- Disable the Break key (Including CTRL break).
- Open a Password window when specific applications or directories are run or opened.
- Prevent users renaming files.
- Disable the F12 escape route from the desktop.
- Prevent TaskWindows from being opened.
- Disable the Alt-break key combination (OS 3.5 or later).
- Prevent files being copied without the master password.
- Prevent disks from being renamed.
- Prevent configuration being changed with *Configure.
- Prevent computer operating if it is started with the SHIFT key held down (RiscPC/A7000 only).
- Prevent users running some filetypes (for example Obey Files).
- Grey out the Task Manager icon.

DeskLock is completely transparent in use and will not interfere with any other operations on the computer. A user will be able to load and run applications and open any directories that they are allowed to. Should a user try to copy a file or open a protected app or directory then the appropriate password window will open on screen.

A Password window

This is an example PassWord window.



This particular window will open when a user tries to open a passworded directory. The computer will now be locked. The user will have to type in the correct password for the directory. If they get the password wrong then the directory window will not open. While the PassWord window is on screen the mouse will not function and windows cannot be moved or closed. Once a password is entered the computer will un-lock and become usable again.

An application Password window will open when a user tries to run a protected application. If the wrong password is entered then the application will not run. With filer operations (copying files) a PassWord window will also open. A wrong password means that files are not copied.

Master Password

In order to quit DeskLock you will need the master password. By default this is:

PassWord

Note that with DeskLock all passwords are case sensitive. This means that "PassWord" is correct. However typing "Password" will be incorrect.

The master password can be changed using the DeskPass application, this is covered later in the manual. If you do alter the master password (and we strongly recommend that you do) then write down the new password and keep it safe.

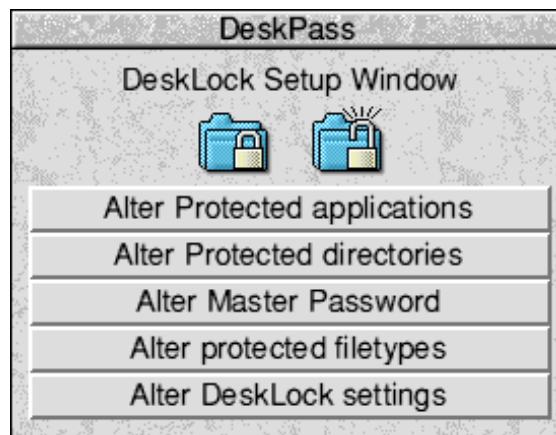
Also keep a list of passwords for particular applications and directories somewhere safe, but not with the master password.

Quitting DeskLock

If you do need to quit DeskLock then you will need to enter the master password. If the wrong password is entered then DeskLock will refuse to quit.

DeskPass

DeskPass is the application that is used to set DeskLock. In order to run DeskPass you will need to quit DeskLock.

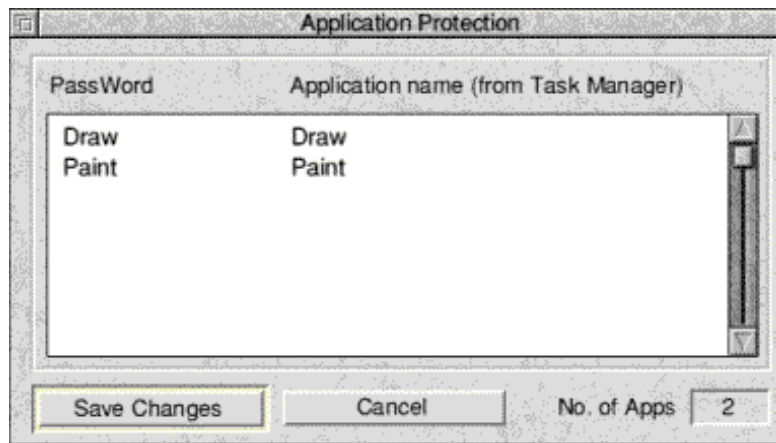


This is the DeskPass main window. As you can see it has five buttons. Each of these will lead to another window that allows you to set up DeskLock.

We recommend that you do not install DeskPass onto any of the computers you are protecting. Instead copy Desk Pass to a floppy disk and use it from there. Once you have set up a computer you should only need DeskPass to alter a password.

Protected applications

Clicking on the "Alter Protected applications" button will open the protected application window.



This window shows you the names of all protected apps along with their passwords. This window also shows you the current number of protected apps.

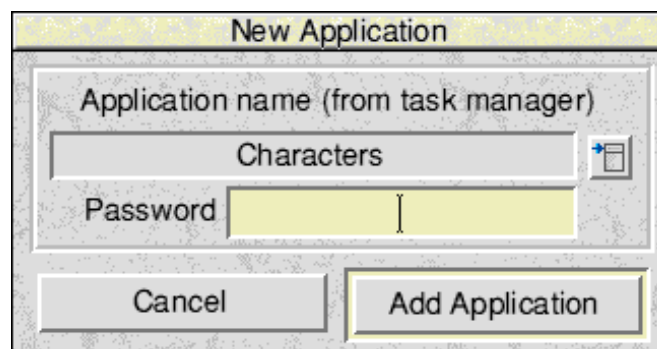
Clicking on "Save Changes" will save the current list of protected applications into DeskLock and close the window.

Clicking on "Cancel" will discard any changes made and re-load the old list of protected applications.

Adding an application

Adding an application to the list of those that is protected is very easy. Simply drag the application (e.g. !Chars) into the window.

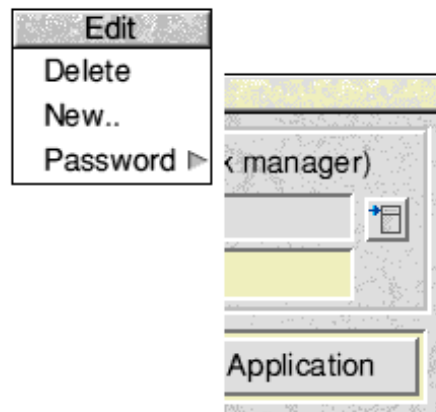
DeskPass will then load the application under controlled conditions and work out its internal name (as displayed by the Task Manager). Then the "New Application" window will open.



As you can see this window has the internal name of the application shown in an icon. You can now type in a password for this application. Clicking on the "Add Application" button will add this app to the list. Clicking on "Cancel" will not add the application.

You can also add an application to the list of those that are protected manually. To do this load the application

that you want to protect onto the icon bar. Go to the DeskPass "Protected applications" window and click MENU. Click on "New.."



The new application window will now open. On the right side of the window is a menu button. Clicking on this will open a menu showing all the currently running applications. Choose the application you want to protect from the menu & click on it.

You can now type in a password & click on the "Add Application" button in the same way as shown on the previous page.

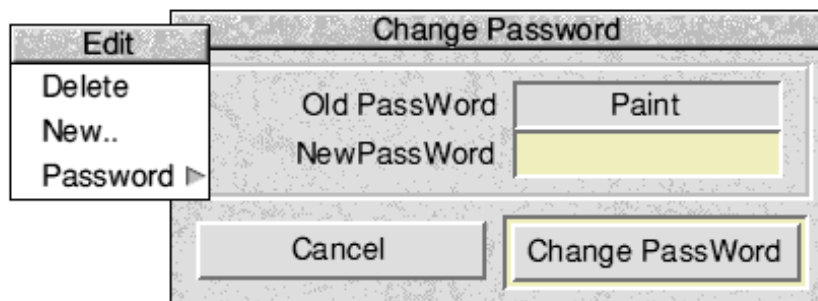
Once you have added all the apps you need to don't forget to click on the "Save Changes" button in the "Application Protection" window.

Deleting an application

You can delete an application from the list that is protected using the "Delete" option on the menu. If you delete an application by mistake click on "Cancel" in the "Application Protection" window.

Changing Passwords

As you can see from the previous page the "Application Protection" menu also has a Password option.

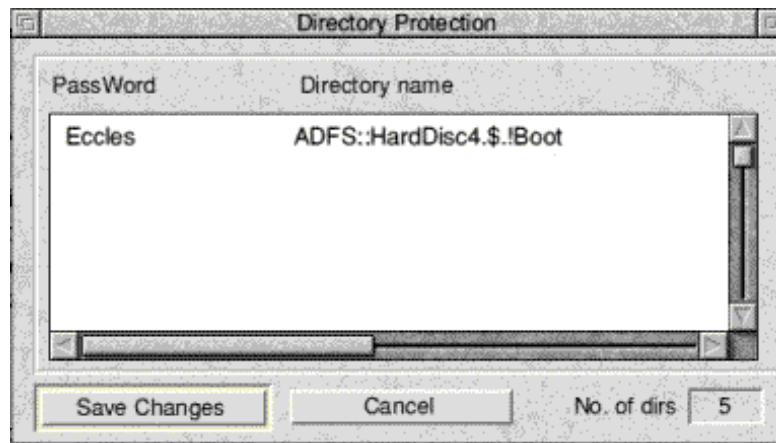


This leads to a window that allows you to change the password for an application. To change an applications password just click MENU over the applications name in the list and then go past the "Password" option.

Clicking "Change PassWord" will change the password, clicking on "Cancel" will leave the password unchanged.

Protecting directories

Clicking on "Alter Protected directories" from the main window will open the "Directory Protection" window.



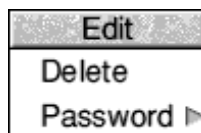
This window works in the same way as the "Application Protection" window. You drag a directory into this window then give it a password. You can see in the example above that the directory:

ADFS::HardDisc4.\$.!Boot

has been given the password "Eccles".

This means that if any user tries to open the !Boot directory with the SHIFT key they will have to enter this password. If they do not know this password then the directory will not open.

The "Directory Protection" window also has a similar menu to the "Application Protection" window. From the menu you can delete a directory and also change the password for an existing directory.



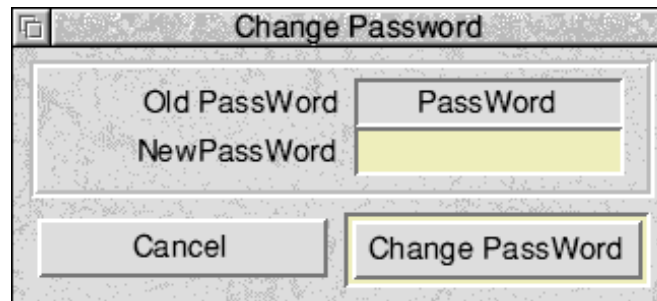
You must always have at least 1 protected directory in the list. If you try and delete the last directory DeskPass will not allow it.

Normally if directories are protected and a user renames them then the password feature will not work. To prevent this ensure that the "Protect file operations" button is selected in the "DeskPass Settings" window. This will prevent a user renaming a directory (as well as copying it under a different name).

DeskLock will also automatically protect itself and any copies of DeskPass that a user may obtain. DeskLock will prevent a user trying to open itself (with SELECT+SHIFT) and will also prevent a user running or opening a copy of DeskPass.

Alter Master Password

Clicking on the "Alter Master Password" button on the DeskPass main window will open the "Change Password" window.

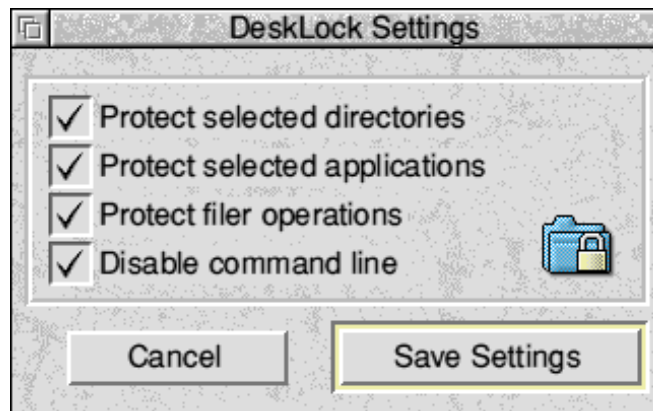


As you can see the illustration above shows the default master password "PassWord". You can type in the new password in the icon provided and click on "Change Password" to change the password. DeskPass will prompt you to ensure you have typed it correctly. If you confirm that you have then the new master password will be automatically saved into DeskLock.

We very strongly recommend that you change from the default master password "PassWord" to a password of your own choosing as a matter of urgency. Leaving the password unchanged will greatly limit the security of DeskLock because anyone reading the manual will be able to see the password, use it and disable DeskLock.

DeskLock Settings

Clicking on the "Alter DeskLock settings" button will open the settings window.



Protect selected directories

This button must be selected for the password directory protection to be activated. If this button is off and a user opens a protected directory they will be allowed access.

Protect selected applications

This button must be selected for the application protection to be activated. If this button is off then users will be able to run any application they please.

Protect filer operations

If this button is selected then in order to copy files a user will need the master password. When a file is dragged from one filer window to another a password window will open. If the master password is not entered then the file will not be copied. Selecting this button will also disable the following *(star) commands.

- *NameDisc
- *NameDisk
- *AddTinyDir
- *Rename
- *Configure

Disable command line

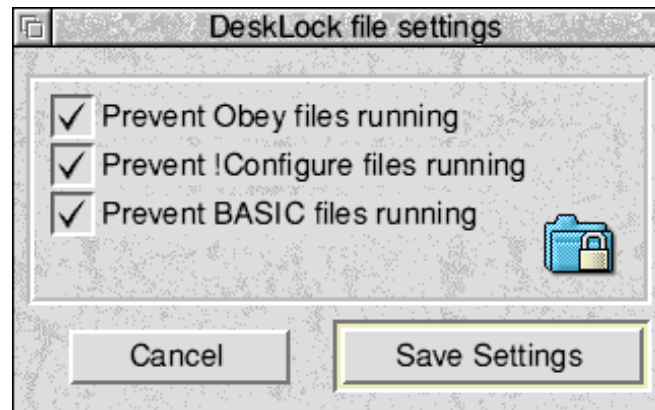
If this option is selected then then the F12 key and the *Commands entry from the Task Manager window will be disabled. Any attempt from the user to exit to the command line will be met with an error box.

Automatic settings

DeskLock will also automatically disable the Break key, prevent the ALT-Break key combination from killing apps on RISC OS 3.5 or later and also disable Task Windows.

Protected filetypes

DeskLock has the facility to prevent some types of files from being run with a double click.

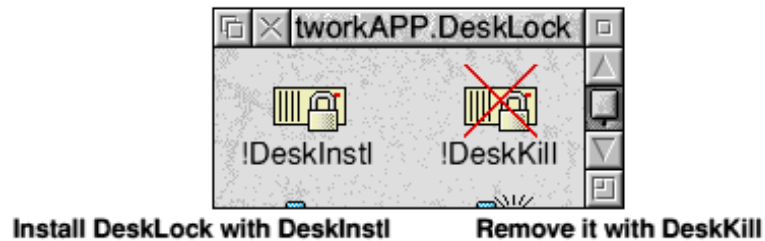


These settings will have no effect on the running of legitimate applications. However they can be used to prevent users writing BASIC or Obey files in an attempt to defeat DeskLock. If a users tries to run an Obey file and the "Prevent Obey files running" button is selected then they will be asked for the master password. Without the correct password the file will not run.

Removing Desklock

As we have seen before the automatic installer works by adding a line to the !System.!Boot file and placing a copy of DeskLock into the !System folder.

If you do need to remove DeskLock from a computer then we recommend that you use the application !DeskKill to completely remove all traces of DeskLock from the machine.



Any attempt to remove DeskLock manually will most likely result in a locked computer and we strongly recommend you don't try a manual removal

Obviously you need to ensure that DeskKill is not installed on a computers hard disk. If, due to interference by users, you do discover a locked machine then you will need to attempt to run DeskKill. If you have locked the CMOS RAM on your computer then you will need to unlock it before running DeskKill.

A note about Protection

DeskLock can provide a high degree of security for data and applications however we suggest that you take note of the following.

DeskLock can only protect a computer if it is loaded. This is why we provide an installer that attaches DeskLock to the computers !System folder and alters the !System.!Boot file to automatically load DeskLock every time the system folder is "seen" by the computer.

We recommend that you change the master password on a regular basis. Just in case someone manages to discover what the password is. All passwords are stored inside the DeskLock application in an encrypted form.

If you do forget the master password then you may well experience difficulties. Write it down somewhere safe. If you forget other passwords this is not so important as you can always use the DeskPass application to find out what the other passwords are. Without the master password you may end up having to reformat the harddisc and re-install all your applications.

FS Lock (!Configure)

Under RISC OS 3.5 or later the !Configure application has an option to lock a machine. This prevents the CMOS Ram from being altered or files being copied to the hard disk.

If your machine is locked in this way then we recommend that you unlock it and instead use the improved security provided by DeskLock.

If you use the !Configure locking system then users will be able to turn on the computer holding down the SHIFT key and hence by-pass the normal boot sequence. This will obviously result in DeskLock not being loaded. Since DeskLock prevents a machine starting if SHIFT is held down this would be counter productive.

It is also possible that the machine may boot after having been locked but that the keyboard and mouse will become inoperative. We therefore strongly suggest that you do not try and use the !Configure locking system and DeskLock together.

DeskLock and Zap

We do not recommend that you have a copy of the text editor !Zap installed on any computer that is running desklock without having !Zap password protected. If a user manages to load a copy of Zap they will be able to open a task window and hence may be able to break the DeskLock protection system.

If you do have a copy of Zap then ensure that it has a DeskLock password and that users do not know this password. This ensures that they will be unable to load it.

Here are just a few of the other products you will be able to
download from RISCOS.com free of charge
(You can make a donation to help support future product releases but this is entirely voluntary)



This Documentation is © 3QD Developments Ltd 2026
Some of the products shown above might not be available immediately.
Not all products will run on all versions of RISC OS, check the product information page for details.

Other Products list last updated 29/2/26