



**DMH Manual
Version 1.4**

© 2004,2005 DeadMan's Handle Ltd

Contents

| | |
|------------------------------------|-----------|
| Part 1 Introduction | 4 |
| 1 Dead Man's Handle | 4 |
| 2 Introduction | 4 |
| 3 System Requirements | 5 |
| Part 2 Fast Setup | 7 |
| 1 Installation | 7 |
| 2 Three Steps | 9 |
| Part 3 Configuration System | 13 |
| 1 Background | 13 |
| 2 Basic Tab | 15 |
| 3 Challenge Tab | 20 |
| 4 Extra Files Tab | 27 |
| 5 Advanced Tab | 29 |
| 6 Select Folder | 37 |
| 7 Select Screen | 40 |
| 8 Select File | 43 |
| 9 Exit Messages | 45 |
| Part 4 Activation | 47 |
| 1 Boot up and Log On | 47 |
| 2 Challenge Screens | 49 |
| 3 Deletion Approach | 51 |
| 4 Panic Button | 52 |
| Part 5 Useful Information | 55 |
| 1 Extra File Information | 55 |
| 2 Security Levels | 56 |
| 3 Installation Defaults | 59 |
| 4 Passwords | 60 |
| 5 Random Number Files | 60 |
| 6 Usage Information | 61 |
| Part 6 Support | 64 |
| 1 Support | 64 |
| 2 Credits | 64 |

| | |
|--------------|-----------|
| Index | 65 |
|--------------|-----------|

Part

1

1 Introduction

1.1 Dead Man's Handle

Thank you for purchasing Dead Man's Handle (DMH), a new concept in notebook or laptop security. This utility will defend your machine even when it has been lost or stolen. If you want to just get started, then simply follow the [installation](#) instructions and then carry out the [three steps](#) to quickly configure it. If you want to know more about DMH, then a good place to start is the [Introduction](#).

After the introduction, you will find lots of detail in the help file and the manual (both of which are closely related). You can always get support at:

web address: www.deadmanshandle.com
mail address: support@deadmanshandle.com

We have also provided an FAQ, other white papers and support tools, either on the disk (if supplied) or on our [web site](#). The web site will always have the latest versions of all these items, and provides other resources as well.

If you have any comments or problems with any aspect of this software or its documentation, please do not hesitate to contact us.

*The DMH Development Team
Dead Man's Handle Ltd*

1.2 Introduction

DeadMan's Handle refers to an old train device: the dead man's handle. It was typically some form of switch that the driver would keep closed. Should he suffer a calamity - such as a heart attack - his hand would loosen and the switch would open, stopping the train automatically. The aim of the dead man's handle was to protect the passengers, even in the worst possible case.

DeadMan's Handle tries to do the same for your information. Should the worst happen and your notebook be lost or stolen, DeadMan's Handle will try to ensure that your confidential information does not fall into inquisitive hands. Once you have set it up, each time you - or the thief - boots up and logs on (depending on your setup) there will be an innocuous-looking challenge. Fail the challenge and the system will quietly delete the files you have told it to and then delete itself, removing any audit trail. Whoever has your machine probably will never know the information was on it.

Benefits of DMH

DMH protects your information even if you have lost control of your notebook. Thus it can:

1. Save you loss of business due to information exposure.
2. Protect you from legal difficulties due to loss of information about clients, suppliers or contacts.
3. Save you from general embarrassment or loss of professional credibility.
4. Provide an extra level of security to your information protection strategy.
5. Show evidence of good corporate governance.
6. Help you meet Governmental requirements such as Data Protection laws.

DMH Features

1. Highly customizable: you can vary many of the system parameters.
2. Turns your notebook or laptop into a trap for unwary attackers.
3. Select your own challenge screens (including both text and graphics challenges) and create your own screens if you wish.
4. Allows automatic challenge, or challenge at log on.
5. File deletion to five different security standards, one of them military and one to the most

- 6. exacting file deletion specification yet given.
- 7. Extreme ease in installation and setup.
- 8. Panic button capability – the system can be manually activated from the system tray, for that emergency deletion.
- 9. Deleted files will have their names altered, their date stamps randomized, the file contents and slack space will be overwritten, and files will be truncated to 0 bytes: all integrating to make recovery and audit extremely difficult.
- 10. Swap file cleanup on NT/2000/XP/2003 systems.
- 11. Self-deletion on activation, removing all traces of its existence.
- 12. Protects itself from interruption when active.
- 13. First-rate context-sensitive help.
- 14. Product support provided by [web site](#) and [eMail](#).
- 15. Advanced encryption and random number generation technology.
- 16. Completely compatible with encryption utilities.
- 17. Developed to Government standards, and is internally fully documented.
- 18. Works on Windows 95, 98, Me, NT, 2000, 2003 and XP (some capabilities vary depending on the operating system).
- 19. Special tools are available for registered customers, to help manage large scale distribution across systems and other tasks.

There is one very important thing you must do: backup your information. If DMH is activated it will try to destroy the nominated files: probably your most sensitive information. It will not be recoverable unless you have backups. And, of course, do not keep your backups with your notebook.

We also recommend that you give DMH a trial run or two: get used to using the system. This will reduce the probability of mistakes in the future.

1.3 System Requirements

The following are the minimum requirements for installing and using DMH.

Systems

Windows 95 (this should be running Internet Explorer 4.0 or later)
Windows 98
Windows Me
Windows NT (Service Pack 6, running Internet Explorer 4.0 or later)
Windows 2000
Windows XP
Windows 2003

Please note that not all of DMH's capabilities are available for [earlier](#) operating systems.

Memory

Windows 95, 98, Me and NT: 64MB.
Windows 2000, 2003 and XP: 128MB.

Version

This help file covers the Version 1.4 release of DeadMan's Handle.

Part

2

2 Fast Setup

2.1 Installation

To commence installation, ensure that you are signed on to an Administrator level account. If you have been sent a CD, simply place the provided CD into your drive. It should autostart and present you with options, one of which is to start the installer. If it does not, then simply run the program DMHInstaller.exe.

If you have downloaded the distribution kit from the Internet, first unzip it to any temporary folder on your system. There will be one executable file: DMHInstaller.exe (DMHInstallerTL.exe for the time-limited version). Run this program - you can just double-click on the file in the Windows Explorer.

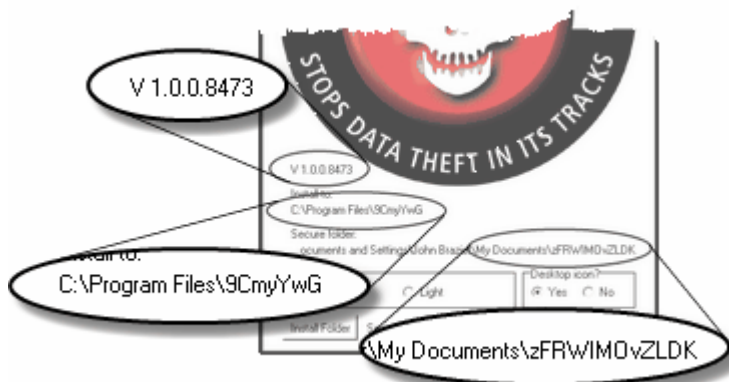
In either case, once you have run the installer you will see the installation screen:



The installer has already determined a default installation configuration. You can, if you wish, just press the Install button. You can make changes to all the options at a later time. However the screen does provide some information and options that you can implement straight away.

Important Information

Directly below the logo on the installation screen are three important items of information:



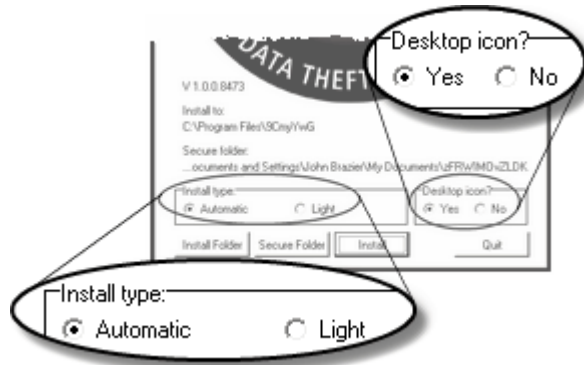
1. The first is the DMH version number - which will be later than the one shown.
2. The second is the proposed installation folder. This will be a random folder name in the

- Program Files folder.
- The third is the proposed secure folder. This will be a random name in the "My Documents" folder.

The installation and secure folder are given random names on purpose. This can make them harder for an attacker to identify (even though they will be renamed in the DMH deletion process anyway), but the aim is for you to rename them to something meaningful to you. The secure folder is created so that DMH is pointing to a known empty folder. If you wish, you can alter either of the proposed installation folders (see below).

Installation Options

Beneath the folder information are the possible installation options:

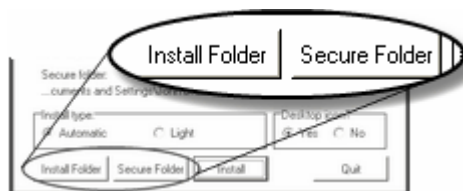


The first governs the type of installation: "Automatic" or "Light". The Automatic installation means that you will get the version of the DMH [configuration system](#) that lets you select its [appearance](#). The Light installation provides a configuration system without skin support. This second option is forced for Windows 95 and NT systems: you cannot change it. However, you can select a Light installation on the other systems if you wish (the configuration system is smaller in the Light version).

Note: the capabilities of the DMH are identical for any given operating system in the two versions (except for the appearance of the configuration system). All the deletion and other capabilities are driven by the [operating system](#), not the version of the DMH that you install.

The second option allows you to place a link to the configuration system on your desktop (it is always added to your start menu). We do not especially recommend this option, and this is covered further in one of the white papers. Note that the [panic button](#) is always placed in the system tray.

The other settings you can change are the installation or secure folders:



The two buttons in the bottom-left corner of the window let you change the installation or secure folder respectively. Pressing either button brings up a simple [requester](#) that allows you to select or create the appropriate folder (this is a simplified version of the requester that appears in other parts of the system). For quick instructions on how to use it, see [step 1](#) of the [Three Steps](#) section.

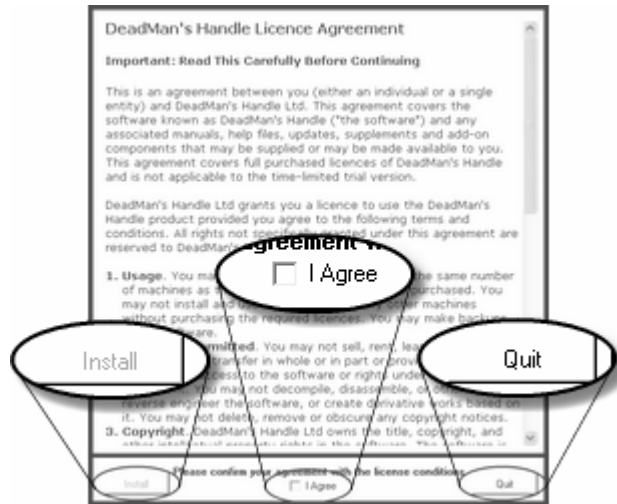
The last two buttons on the screen let you quit the installation, or go ahead with the installation with your settings:



If you press Install, DMH will then move on to the next stage.

End User Licence Agreement

DMH will then present you with the following screen, which has the licensing agreement:



If you press the Quit button you will exit the installer. The Install button is greyed out - you must read the agreement and then click in the "I Agree" box. The Install button will activate and if you press it then DMH will install itself and leave you in the configuration screen, ready for the last part of the installation covered in the [Three Steps](#) section. As soon as you see the configuration screen you can investigate the settings.

2.2 Three Steps ...

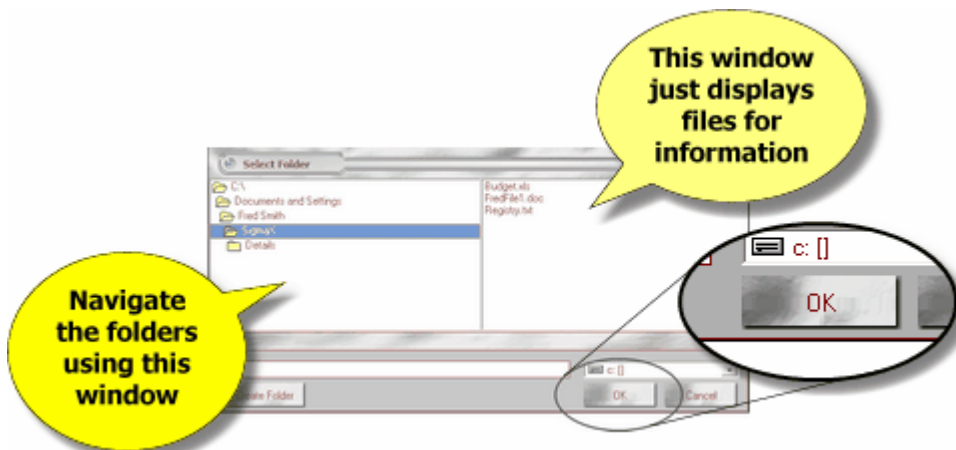
After [installation](#), you will be placed in the DMH configuration screen - it will look like something like these below, but you can change what the screens look like at any time. This section will give you a configured system in three easy steps.

Step 1

On the Basic tab, select the folder you want to be secured by using the Select Folder button - if you want to change it (otherwise you can skip this step). This will be the folder that DMH will attempt to delete when activated. You had an option to select this folder during the installation, but you can change it at any time. Do not select the system drive (such as "C:\"): this will lead to trouble if DMH is ever activated as DMH will start deleting the operating system, which will stop the computer at some point.



If you hit Select Folder, you will be sent to a folder request screen:

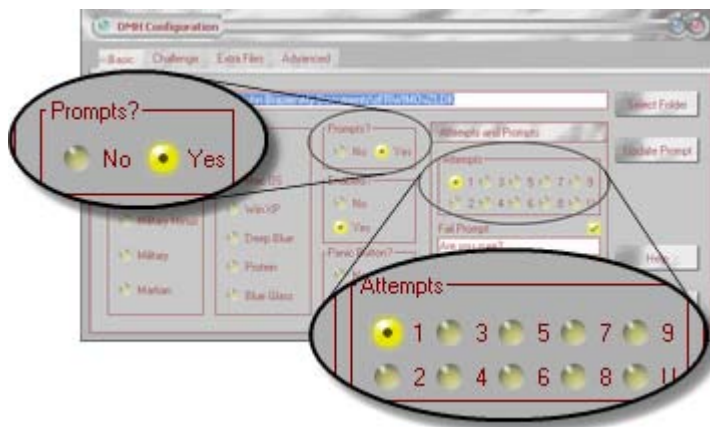


The upper-left window shows the folders: single-click on a folder to open it; double-click to select it as your target deletion folder. If you have a folder open, pressing the OK button will also select it. The right-hand window shows the files in any folder and is for information purposes only. If you need to create a folder, then see information on the [create folder](#) button. Above the OK button is a [drive selector](#) - do not use it to select a network drive!

After you have selected your folder you will be returned to the Basic tab on the main screen with the folder listed in the Secure Folder field.

Step 2

If you fail the challenge, DMH will immediately delete the selected files. If you want to give yourself a chance while you are experimenting with the system, simply say Yes to the Prompts? option (still on the basic tab). The Attempts and Prompts panel will open:

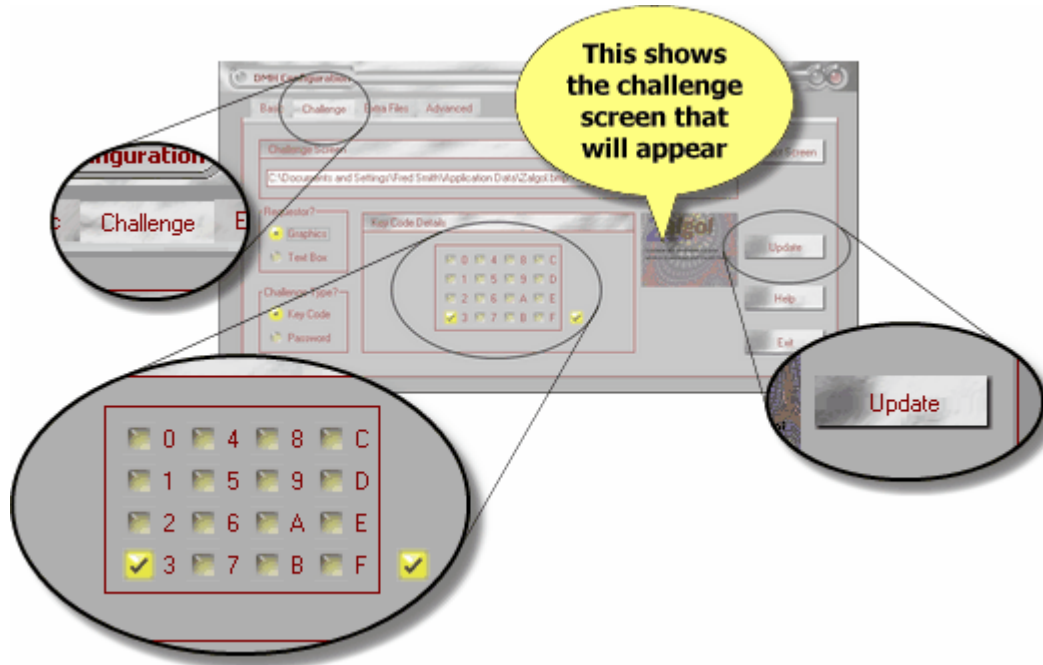


Now give yourself a few tries (say 3 or 4). This means that when you are presented with the

challenge, you will get that number of attempts before the deletion process is invoked.

Step 3

Click on the [Challenge tab](#) and you will find a [challenge screen](#) selected, which is the screen that will appear at your next bootup/login. What you now need to do is set up is your key code:



It is set up for a single key code: currently 3, which is ticked, and the whole key code box is ticked to show that the system knows the value. Tick (or untick) as many codes as you wish (so you could have none ticked, or 1 and 2, or even all of them - any combination is legal), and press the Update button. Remember your key code: you will need it the next time you boot up and log on to your machine.

Press the Exit button. The next time your [machine starts up](#) you will be presented with the [challenge screen](#) when you log on, and the [panic button](#) will appear in your system tray. Enter your key code and press OK - that is all that needs to be done. Note: if you accidentally changed something and did not press the relevant update button you will get an [exit message](#).

Notes

Do not forget: enter the wrong key code - or press Cancel - and DMH will activate (unless you've given yourself some extra tries). It will shred the folder you have selected. So keep backups!

Lastly, you have a large number of options as to how DMH is configured. You will find it worthwhile to ultimately read the whole of this manual (or help file) to get the best usage out of the program. For now, we strongly recommend that you review the following sections: [Boot up and Log On](#), [Challenge Screens](#), [Extra File Information](#), [Security Levels](#), [Passwords](#), [Usage Information](#) and [Random Number Files](#). You may well wish to modify your DMH configuration after reading this information.

After Installation

After the installation, you should archive off the DMH distribution kit to a CD or some other backup system. When DMH is activated it will not delete the distribution kit if it is still on your system, which is a giveaway that DMH was present. One of the aims of DMH is that there is no obvious trace left that it was on your machine.

Part

3

3 Configuration System

3.1 Background

Screens

The configuration system of the DMH is the core of the system. Aside from this utility, there are only two other visible components:

1. The [panic button](#), which is used to delete your selected files in an emergency.
2. The [challenge screen](#), which appears when you fire up your system.

Otherwise, the configuration utility defines all the rest of the DMH system. You access it by selecting it from the Start menu, or by double-clicking its shortcut if you placed one on your desktop. This section describes this system.

Important: the configuration utility accesses system registry keys. Because of this, it will only function correctly under an Administration level account.

Title Bar

Before going on to the details of the individual configuration screens and their options, a few general points should be discussed. At the top of the utility there is the title bar, which looks like so:



The title bar is visible in all the configuration screens. It has four features, going from left to right:



1. A green system menu button at the top-left;
2. The title "DMH Configuration";
3. A blue help button; and
4. A red close button.

The green and red buttons both allow you to shut down the DMH configuration utility; it has been set up so that it cannot be resized. The blue button calls up the system help in the same way as if you press any button labelled Help.

The title bar shown above is for the default appearance of the utility - you can change this by going to the [Basic tab](#). If you do alter the appearance of the utility the title bar will look different and the colours will change. However, the four basic features shown above will still be in their same positions and their icons will be self-explanatory.

Configurations

The next point is that the utility does not require the loading and saving of configurations. The current configuration is acquired when you start it and each time you do something it is saved in real time. This is for simplicity of use, and means that everything you see in the DMH screens correctly shows the current configuration, subject to the third point below.

Editing

This third point governs editing. As you will see as you explore the interface further, there are three ways you can do something:

1. You can make a selection from a choice of two or more options. This is always done via radio boxes, looking like so (although there may be more options):



These radio boxes always reflect the current status, and you simply left-click using the mouse on your preferred choice.

2. You have to select a file or folder name. In this case, the system will provide requesters to manage you through the process. When your chosen file name is finally displayed, this will be the name that is held in the system - it will be fully up to date. You can detect this because the fields are display-only: you cannot edit them.
3. You can edit something is by either entering text into a field or selecting from a group of check boxes (see the [key code](#) for more details). In this case, DMH needs to know when you have finished the edit and you need to know if you have confirmed your changes. The mechanism is two-fold: (a) you use an update button by the field to tell DMH you have finished, and (b) each user-alterable field has an update indicator. When you have completed an edit and hit the update button, the indicator by the field will look like this:



What you see matches the configuration database - what has been stored internally. The moment you enter the field and start editing it, then the indicator will turn off:



What you see in the field does not match what is in DMH's database. If you exit DMH without pressing the relevant update button your changes will not be taken - the settings will be as they were before you started the edit. Note that you will be given a [warning](#) in this case.

Lastly, there is one other case when the indicator button may be off: if it is the first time you have tried to edit the field. In this case, the indicator is off to tell you that nothing has been set up on the DMH database for this field (ie you still need to enter something for there to be a value for this field).

Help

DMH supports three types of help:

1. You can always get this help file by either pressing the blue "?" button on the title bar, or by pressing any button marked Help.
2. If you hover over any control, a tooltip will come up to give a very terse description of what the item does.
3. If you right-click on an object, you will usually get a "What's This?" single menu entry. Selecting this will give you a short description of what the item does, and this description will often have links to this help file. You can also get the "What's This?" help on any selected control by pressing the F1 key.

Note: some text controls do not give the "What's This?" when right-clicked. You can still activate the "What's This?" help by pressing the F1 key.

With these general items covered, we can now commence with the first screen on the [Basic tab](#).

3.2 Basic Tab

This section describes the first screen in the DMH configuration utility and provides the absolutely basic configuration functions, which are: (a) the folder that will be deleted when DMH activates; (b) the effectiveness of the deletion; (c) the activation of DMH and the panic button; (d) the user-defined prompt system; and (e) the appearance of the configuration system. The Basic tab shows the following page, which is the default when you fire up DMH:

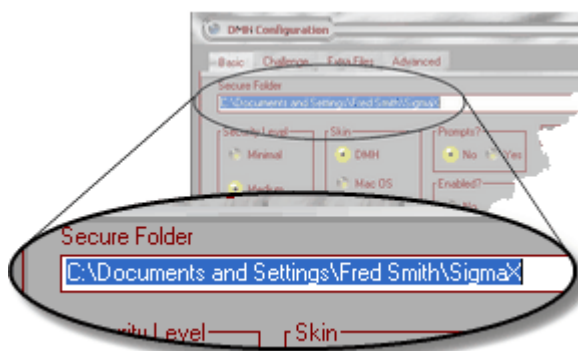


You can always get to this page by clicking the Basic tab:

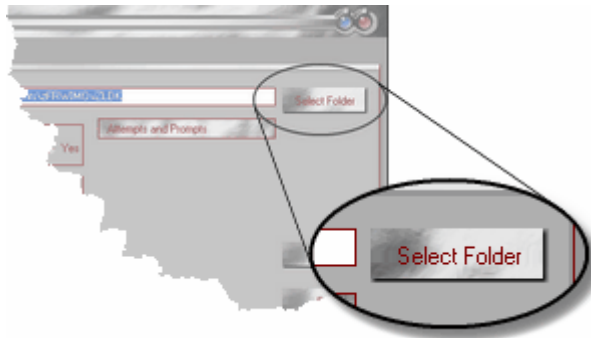


Secure Folder

The first section of this page, underneath the tab, is the Secure Folder field:



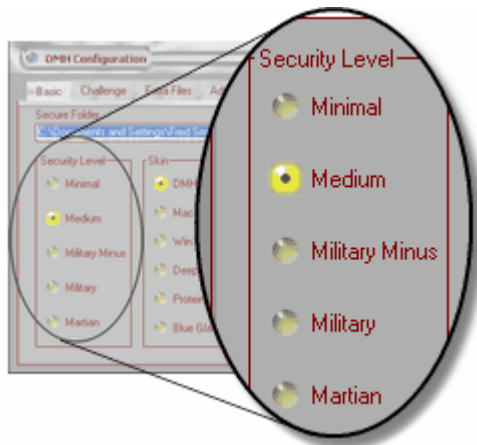
This displays the folder that you have selected for secure deletion: DMH will attempt to delete every file and folder (including the secure folder itself). This field is read-only: you cannot directly edit it. To change your selected folder, simply press the [Select Folder](#) button, where you will be shown the [folder selection screen](#):



Use the folder selection screen as described in the appropriate [section](#). When you have selected the folder you will be returned to this page, with the selected folder shown.

Security Levels

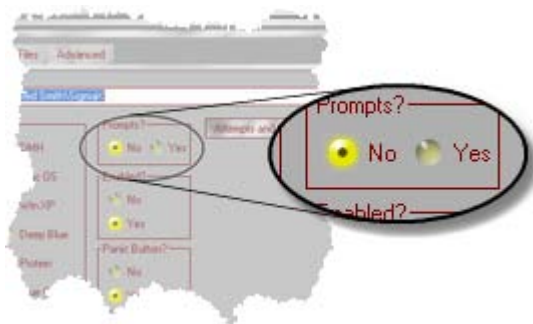
The next part of this page covers the [security levels](#) for the DMH deletion, and looks like this:



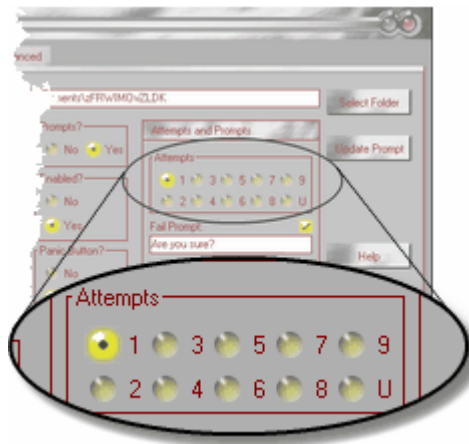
Unless you have specific reasons to alter this setting (please see the [discussion](#) on this), we recommend the default Medium setting. When DMH deletes files at this setting, it carries out one overwrite of the file and its slack space with random numbers, renames the file, randomizes the time-stamps and truncates the file to 0 length before deleting it. We regard this as a good general-purpose compromise between security and speed. To change this setting, simply click on one of the other levels.

Challenge Prompting

By default, when the [challenge](#) is failed DMH will go straight into delete mode. This section of this page allows you to change the default behaviour. You can give yourself a number of tries, and you can create your own prompts. Why you may wish to do this is covered in the [discussion section](#). The switch that manages this feature looks as so:



In its default state (where prompts are set to No), the panel to the right (headed Attempts and Prompts) will be shut. If you select Yes, then the panel will open. This will allow you to do two things. The first is to select the number of attempts that the challenge will give you before invoking the deletion mode automatically:

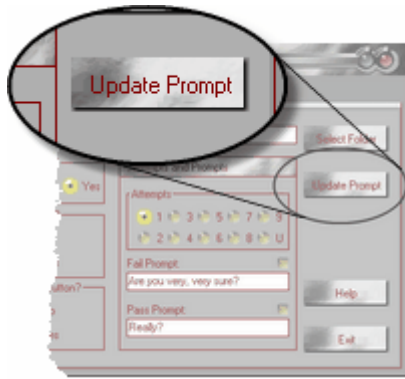


One attempt will still only allow a single attempt, but will display the prompt before activating the delete mode. You may select up to 9 attempts, or 'U', which stands for unlimited tries. In this state DMH will loop indefinitely until the challenge is passed.

You can also define the prompts on this panel, which looks as so:



Note that the default fail prompt is 'Are you sure?', and will be shown when the input you have given the challenge screen is wrong. The default pass prompt is blank (which means that it will not be shown). You may change either of the text fields as you want. If you do, then the check indicators will go out, and you will need to press the Update Prompts button, which appeared when the panel opened:



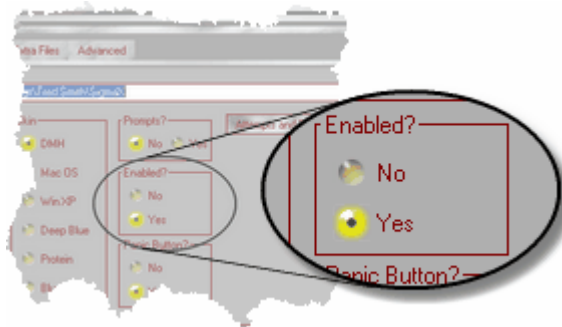
If the information is updated correctly, then the check boxes will light up.

The rules for the prompting are simple:

1. Select the number of tries you require (something like 3 or 4 would probably be the most common).
2. Enter the fail prompt. This will show every time you enter information into the challenge screen that is wrong.
3. The fail prompt will also show if you press the Cancel button on the challenge screen.
4. If you enter something in the pass prompt, then this will be shown if you have put the correct information into the challenge screen.
5. If you leave the pass prompt blank, then it will never be shown: if you have put the correct information in then the challenge system will just pass and exit without activating the deletion process.
6. Each try (failing, cancelling or displaying the passing prompt) counts as one attempt against the attempt limit.

Enable and Disable DMH

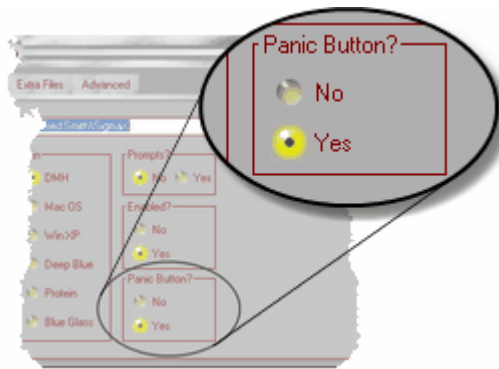
Another part of this page allows you to enable or disable the DMH bootup challenge:



Simply select Yes for enable or No for disable. This is useful if you intend to be at base for a while, in a secure location, and do not want to be challenged each time you start your machine. Do not forget to re-enable DMH when you go out.

Panic Button

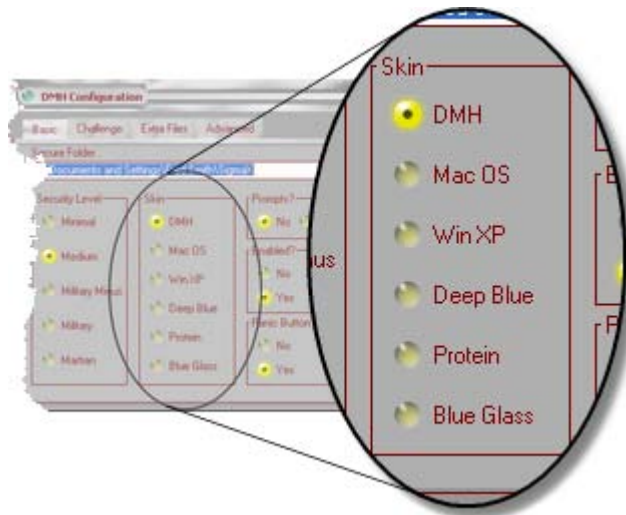
The next part of this page allows you to activate or deactivate the [panic button](#):



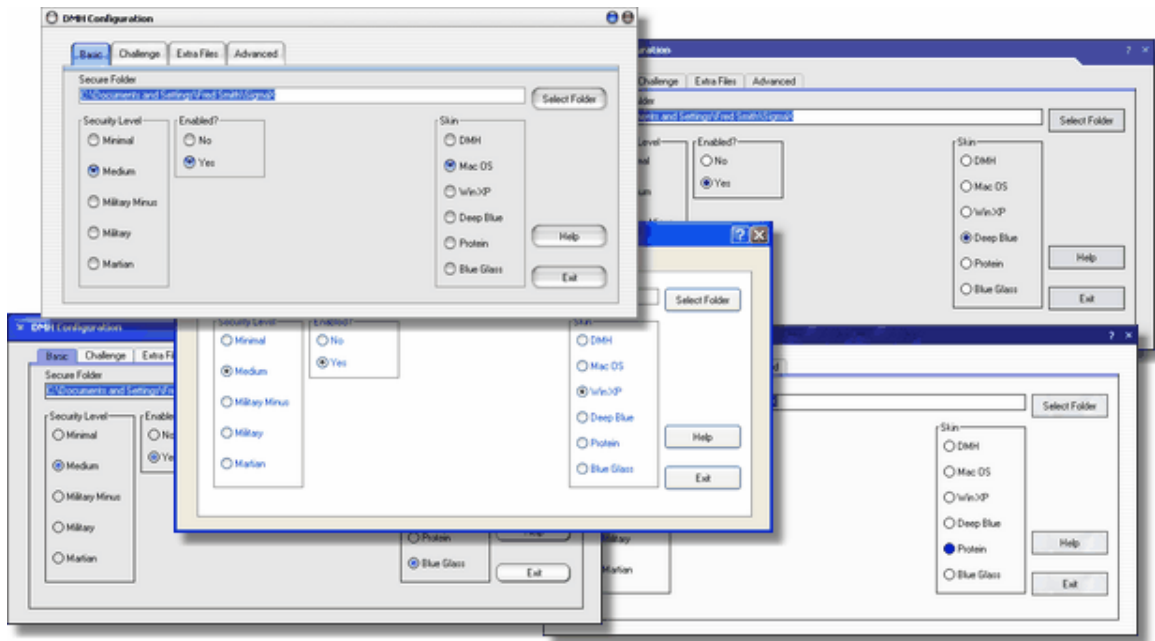
Simply select Yes for enable and No for disable. Again this may be useful if you are to be at base for a time, and do not envisage using the panic button.

DMH Skin

The fifth part of this page covers the visual appearance of the DMH utility, or its skin:



The default skin, called DMH, is the top one in the list. By just clicking on any of the others, you can change the skin to one you prefer. Here is a quick example of the other five:



Help and Exit Buttons

The last part of this page concerns the two standard buttons available on all the pages, in the same location - Help and Exit:



Help gets you to this file (or its electronic version if you are reading the paper manual), and Exit simply exits you from the DMH - no need to confirm. Should you have changed something and not updated it, you will get an [exit message](#).

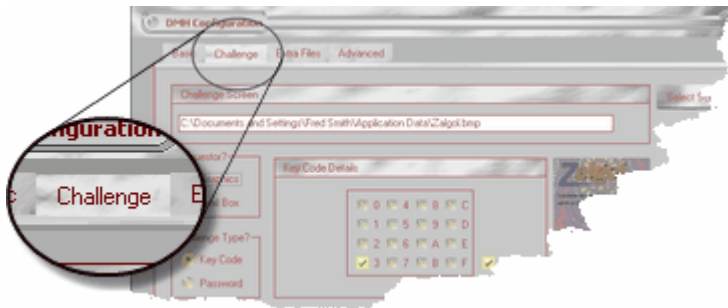
The next section describes the [Challenge tab](#).

3.3 Challenge Tab

This section describes the second page in the DMH configuration utility, which controls the specification of the [challenge screen](#). Basically, you can define what this screen looks like (or what it says) and you can define the type of challenge. The page looks like this when you first go to it:

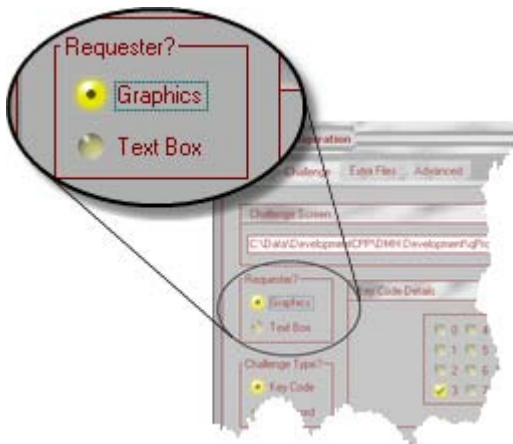


You can always get to this page by clicking the Challenge tab:



Challenge Screen Type, or Requester

This page operates somewhat differently from the Basic page and has more capabilities. The first item to note is the choice you have with regard to the [challenge screen](#), which is labelled Requester:



This option controls half the functionality of this page. It lets you select either a graphical [challenge screen](#), which will be a graphic that you can then select, or a textual [challenge screen](#): this has no graphics, but allows you to specify what text is displayed quickly and easily. You can select your preference by left-clicking on either choice. If you do select Graphics, then you will be shown a thumbnail of what the currently selected graphic looks like:



Graphic Challenge Screen

In addition, the field above the Requester box will be labelled [Challenge Screen](#) and the file name and path of the original graphic file are displayed in the field:



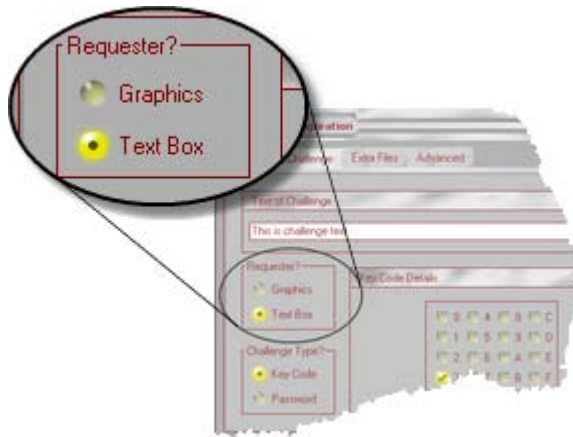
This field is read-only: you cannot directly edit it. To change the selected graphical [challenge screen](#), simply press the Select Screen button and you will be taken to a standard Windows graphical [file requester](#):



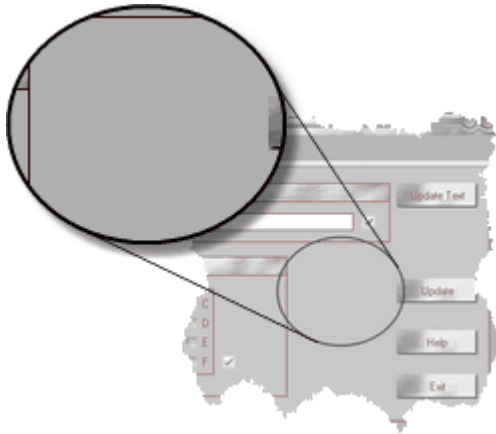
Use the file requester as normal. When you select a file and press OK you will be returned to this page, with the new file shown in the field. Note: the file is actually copied to DMH's home folder and this is the one that is used. The original file path is shown for your convenience. If you were to delete the original file it would not affect DMH as it uses its own copy of the file. A number of graphics screens are included in the distribution kits: we recommend you select one and then archive them off your machine.

Text Challenge Screen

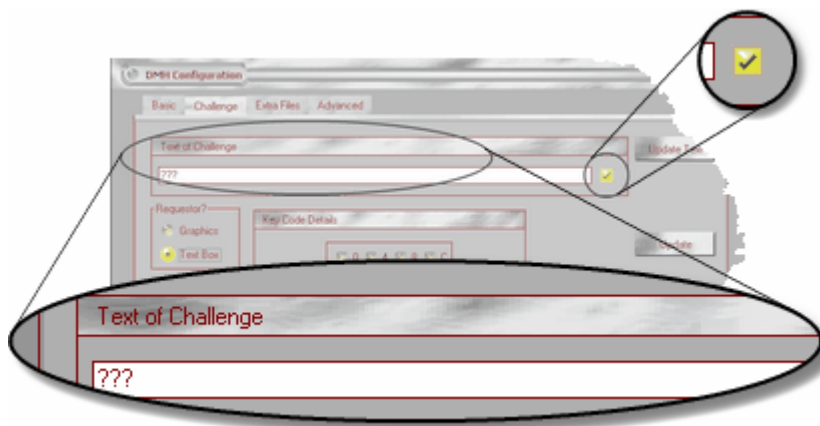
If, on the other hand, you select Text Box from the Requester options, thus:



then the configuration of this page changes. Firstly, the thumbnail disappears:



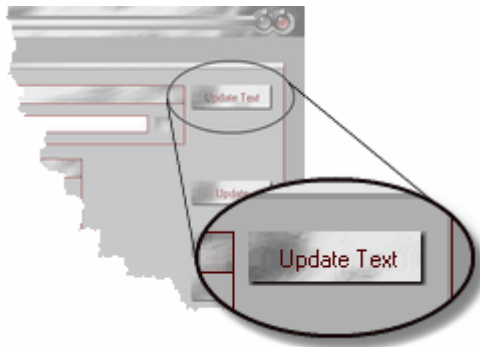
Secondly, the field that was labelled as Challenge Screen is now called [Text of Challenge](#), and when you first see it there will be three question-marks in the field, thus:



Also, note the appearance of the check at the end of the field, which is currently ticked. This means that the system knows about the three question-marks: they have been stored and will appear as your text challenge. This is unlikely to be what you require, so if you want a text challenge then simply click in the field and type whatever text you like. Note that the check goes off when you start editing: that is to tell you that what is in the field now does not match what is in the DMH database.

When you have finished, you may notice that what was the Select Screen button is now labelled

Update Text:



Pressing this button will cause your new text to be taken by DMH. You will see the check box light up to confirm that what you see matches what is in the database. The text you have entered will now be remembered until you change it. If you were to select a graphical [challenge screen](#) for a while and then returned to a text one, you would find the text to be unaltered.

Challenge Type

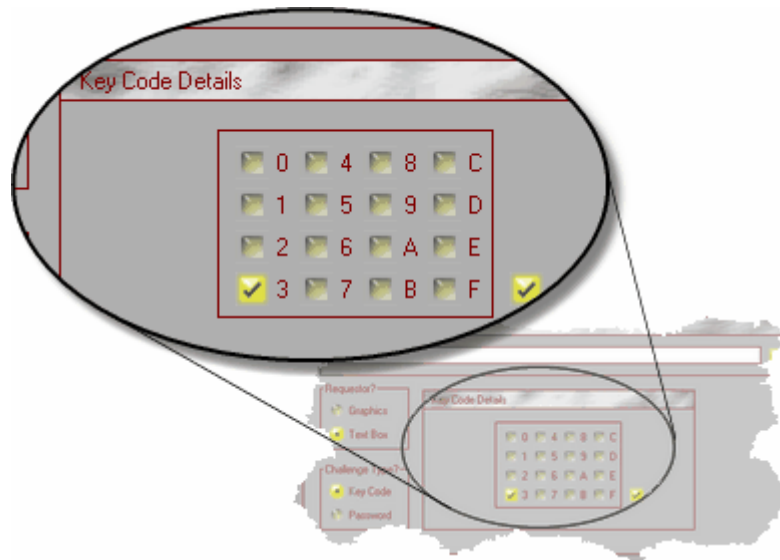
The other half of this page's functionality is driven by the [Challenge Type](#) option:



This option selects the sort of challenge you are presented with on startup. This challenge may be either a key code or a password.

Key Code Challenge

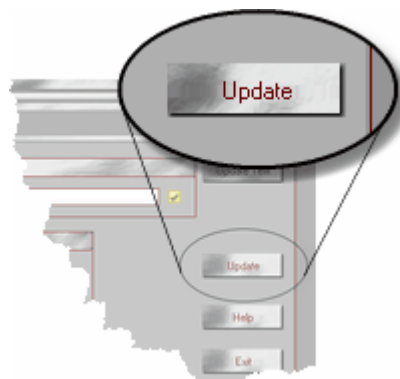
The key code works by selecting a predefined combination of 16 digits; the password is a normal password challenge. The benefit of the keycode mechanism is that you get a pictorial view of the correct input, which many people find easier to remember than a password. You set the key code in the Key Code Details panel to the right of the [Challenge Type](#) option:



The [first time](#) you set the key code details (as covered in the [Three Steps](#) section) it will look like the above, with just the 3 ticked. Note that the status check box is also currently ticked: DMH has stored 3 as the key code. You can tick and untick as many of the boxes as you like for a key code - when you do make changes the status check box will go off as soon as you start. So, for example, the key code 123567 is a valid key code and looks like this:



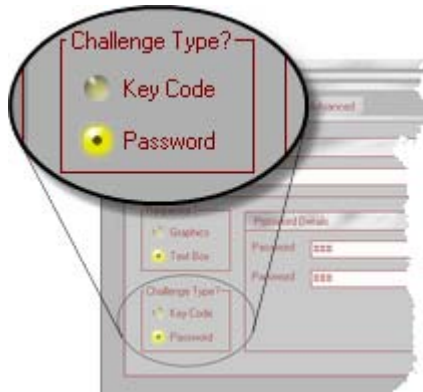
Note that, having selected the key code, the check box to the right of the grid is still clear: DMH has not updated its internal database. To do this simply press the Update button:



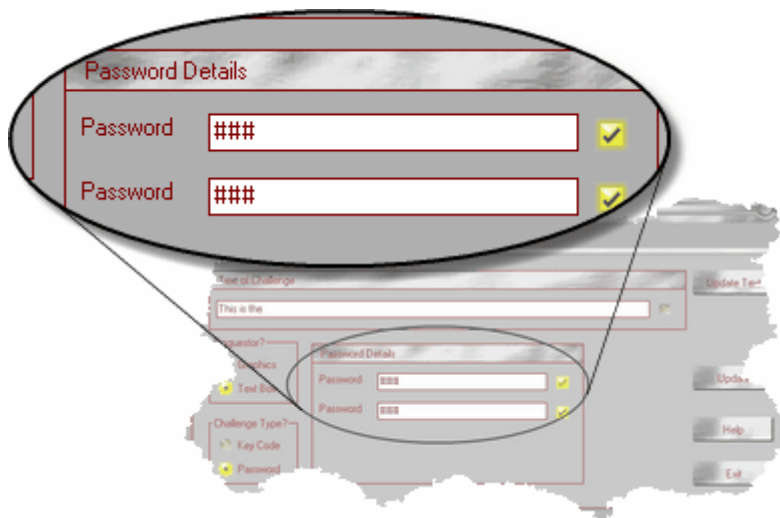
You will find the status check box indicator is ticked to show that DMH has been updated. This key code will be remembered until the next time you change it even if you switch to using a password in the intervening period (see below). All possible key codes are legal: from no ticks to all 16 boxes being ticked. This gives you a total of 65,536 possible codes.

Password Challenge

The other option on the [Challenge Type](#) selector is Password:



When you select it, the Key Code Details panel turns into the Password Details panel, thus:



The [first time](#) you see the Password Details panel, the password will be as shown: it is 3 letters long, is masked and the status check boxes are ticked to show the password is known. This is the [shipped default](#) password, which is "abc". You can actually see this password if you want: a setting in the [Advanced tab](#) lets you have the password displayed rather than having it masked (the idea behind masking the password is that other people cannot see it by looking over your shoulder when you are editing it: it is up to you how secure you want to be). Remember: this is the password you will need to use when you are [challenged](#) the next time you log on/startup your machine.

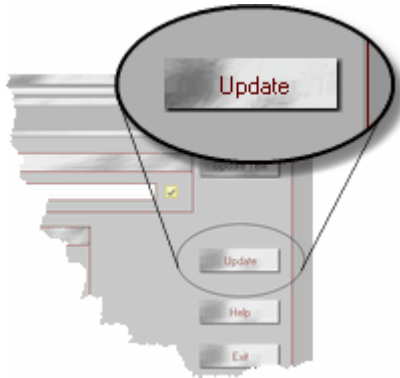
To change the password simply click in the upper field, delete the hashes and then type the new password. Tab to the second field, and repeat the process. You have to put in the password twice as a check to make sure it is spelled correctly (this is especially important if it is masked). The moment you start editing the status check boxes will clear, to show that you are doing an edit. You can have any length password you want (including none at all; see [discussion](#) for comments), all ordinary keyboard characters are included and the password is case-sensitive (this is important).

If you enter two passwords which are of different lengths or are different in their content you will get the following message:



The message states: "The two versions of the password do not match". This should be self-explanatory.

When you have entered the password correctly, twice, confirm you have finished by pressing the same Update button as you would to confirm a key code change:



The check boxes by the password fields will be ticked to confirm that DMH has been updated (assuming the passwords match and other checks are passed). The password will now be remembered until the next time you change it, even if you switch to using key codes during the intervening period.

Help and Exit Buttons

The last pair of items on this page are the standard Help and Exit buttons:

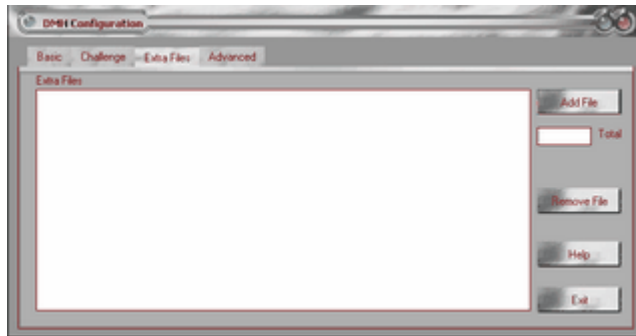


Help gets you to this file (or its electronic version if you are reading the paper manual) and Exit simply exits you from the DMH - no need to confirm. Should you have changed something and not updated it, you will get an [exit message](#).

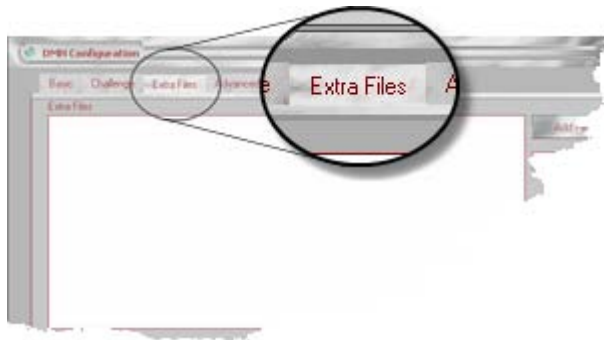
The next section describes the [Extra Files tab](#).

3.4 Extra Files Tab

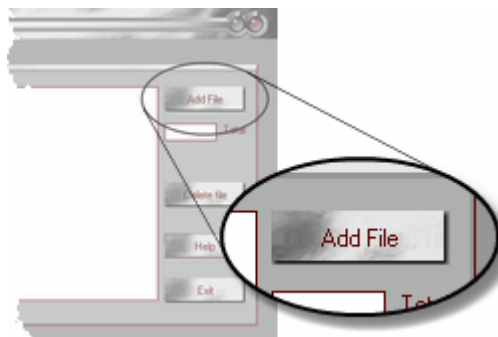
This section describes the third page in the DMH configuration utility, which controls the specification of the [extra files](#). This page allows you to specify other files that you want to be deleted, in addition to the folder you specified in the [Basic tab](#). DMH will also delete these files when activated. The page looks like this:



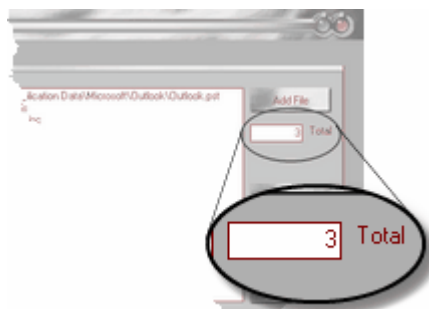
You can always get to this page by clicking the Extra Files tab:



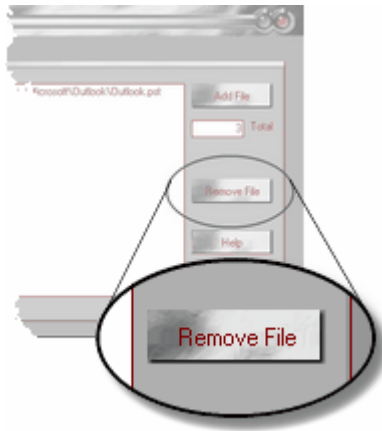
When you first go to this page you will find that no files are listed. Under these conditions DMH will just delete the target folder, with its subfolders, that you specified in the [Basic tab](#). Here you can specify extra files that you want deleted in addition to the secure folder. These might, for example, be [mail files](#). To add a file to the list simply press the Add File button:



Clicking on this button will call up a standard Windows [file requester](#). Use this in the normal manner. When you have selected a file and pressed Open you will be returned to this page, with the file added to the list. Note that the list is always sorted alphabetically and duplicates are simply discarded. You can keep adding files as required and the Total field will keep track of the total number of files listed:



The maximum number of extra files that you can add is dependent on the file name and path lengths, but you should be able to add at least 15 files to the extra files list with no problem; you may be able to add many more. If you wish to remove a file simply highlight it and it will be removed from the list when you press the Remove File button (the file itself, of course, will not be deleted):



You can select blocks of files to delete (by the usual Windows Shift-left clicking mechanism), or you can select several different files at a time by Ctrl-left-clicking on each one, and then clicking on the Delete File button.

Help and Exit Buttons

The last pair of items on this page are the standard Help and Exit buttons, in their normal location:

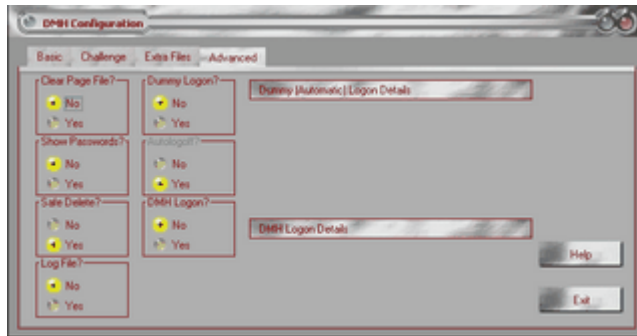


Help gets you to this file (or its electronic version if you are reading the paper manual) and Exit simply exits you from the DMH - no need to confirm. Should you have changed something and not updated it, you will get an [exit message](#).

The next section describes the [Advanced tab](#).

3.5 Advanced Tab

This section covers the fourth and last page in the DMH utility, which controls special settings for the DMH. These are a bit of a mixed bag and have been labelled as "Advanced" because (a) they are fairly specific; (b) will not need to be changed often; and (c) none of them are essential to the functioning of the DMH. Under the Windows 2000/XP/2003 operating systems the page will look like this:



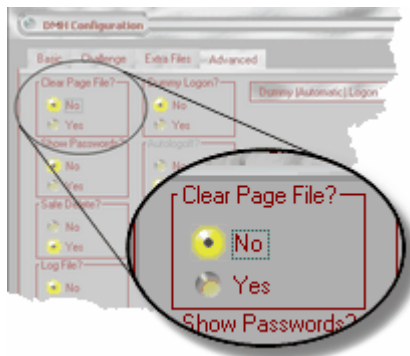
This is the page as it is first seen in its default configuration, as the DMH is shipped. If you are running the Windows 95/98/Me operating systems you will not see the top row of items in this page: these capabilities are either unavailable or not required under these operating systems. NT systems will not have the Dummy Logon option.

You can always get to this page by clicking on the Advanced tab:



Clear Page File

The first item in this page is the one labelled Clear Page File:



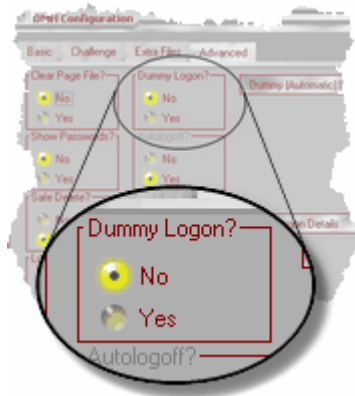
This is set to Yes as the default and only applies to the NT/2000/XP/2003 series of operating systems. What this switch does is tell the operating system to overwrite as much of the page file as possible with zeros each time you shut down your machine. This tends to reduce the amount of information that is left lying around on your machine for hostile people to get hold of (see [discussion](#) for details). Note that this will make your reboots take longer, because your system is cleaning up after itself. You can turn this setting off simply by clicking on No, but remember that it will take one complete boot cycle before the system changes its behaviour (it is a Windows setting that is only changed on boot).

Dummy (Automatic) Logon

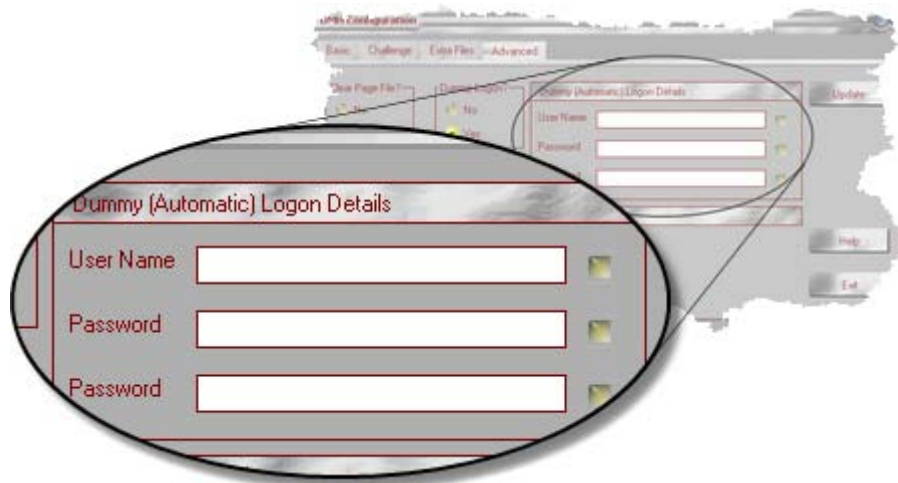
The next item only applies to the 2000/XP/2003 series of operating systems. This is because these

systems will only present the challenge on the first logon after boot (see [discussion](#) for details); so to force the challenge you can set up a dummy account which will cause the challenge to be automatically presented without a logon: the system will sign into the dummy account, present the challenge and on successful completion will log out again allowing you to execute the normal logon. Otherwise the intruder will have to reset a password (typically the Administrator one) to sign on to the system and be presented with the challenge (something that is trivially easily once an attacker has physical access to a machine). It is a matter of personal choice how you would like to proceed, although there are security implications in both cases (this is discussed further in our documents section of the [web site](#)). This switch is not applicable to the Windows 95/98/Me series as log on can effectively be skipped. It is also not available under NT due to limitations on how the logon is handled.

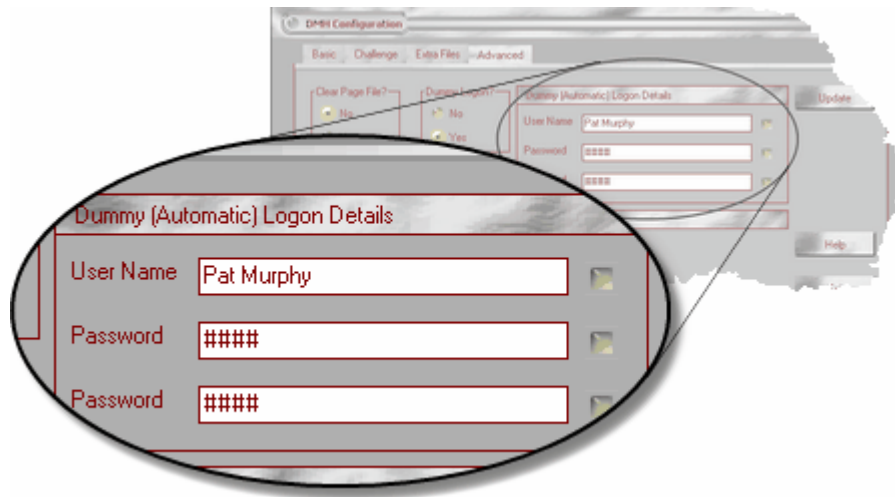
The switch is labelled Dummy Logon and is off in the default case:



You will note that the panel to the right headed Dummy (Automatic) Logon Details is shut. If you click on Yes, the panel to the right will open:



In the worst case, nothing has been set up: there is no user name, no password and no automatic logon. You need to ensure that an account exists and that it has a known password - you may need help from your technical department with this, but see also the [discussion](#). Assuming you have an account set up, then enter the user name and the password (twice) as it will be masked (note that you must enter a password - a blank one is not acceptable to Windows):



You will note the status check boxes to the right of the three fields are off, as the update has not yet taken place. To make the update happen click on the Update button to the right of the panel:



Assuming there are no errors you will find that the status boxes become ticked, to indicate that the update has been accepted. The next time you boot the machine up it should automatically log into the dummy account, present the challenge and if you pass it then it will log out again (see below, and see [discussion](#) for details). You can then log into your normal account as normal. One thing to note about these settings: if you turn off the automatic log off, and then turn it on again, you will find that the name has been remembered but that the password has gone. This is on purpose: it is so that you make sure that you put in the current password for the dummy account - and that you know it. You should always also test that the dummy logon mechanism works before you go out on the road.

There are some further points to notice about this mechanism:

1. DMH has no knowledge of which user name you will use: you may not have created it yet. So any name (including a blank one) will be accepted in the User Name field.
2. If you leave the password fields blank, or enter one and not the other, you will get the following message:



The message states: "Please input the password twice". Just press the OK button to clear it and try again.

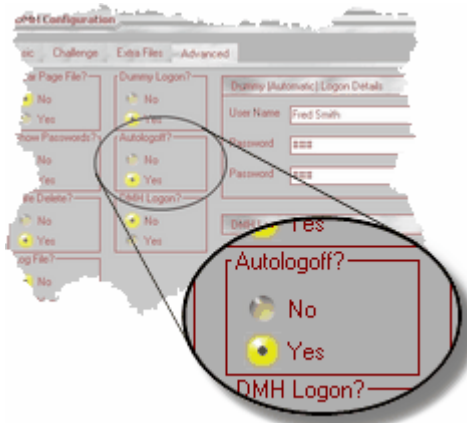
3. If you do enter the password in both fields but they do not match, you will see:



- The message states: "The two versions of the password do not match". Press the button to clear the message and try again.
4. Note that you should use a dummy account for this mechanism: this is because the logout will usually be automatic once the challenge has been passed. The dummy account can be at a lower security level than your actual user account. It is pointless to use it with your live account (you might as well turn off the logon requirement - although this will have security implications for your machine).
 5. Although this mechanism will work under Windows 2003, it may have unintended consequences. Windows 2003 is a server operating system, and depending on its settings this automatic logon into a low privilege account may cause problems.

Autologoff Capability

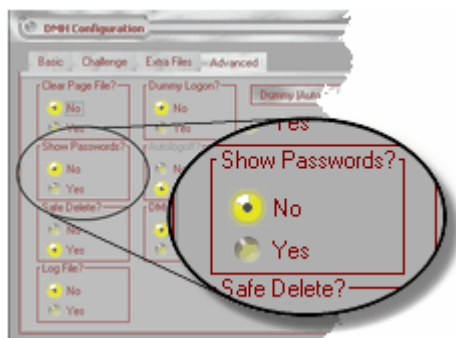
There is also a capability to control the logging off when you are using the dummy account. When you activate the dummy account, the Autologoff radio box becomes activated:



This is a specialized selection, and only applies when the dummy logon is active AND when the challenge has been failed. Under these conditions, if Autologon is set to 'Yes', then the system will sign out and present the logon screen. If not then the user will be left in the dummy account. This is for use with other security software (such as tracking software: see [discussion](#) for details).

Show Passwords

The next item is called Show Passwords:

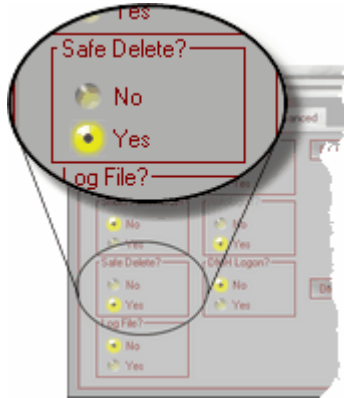


This applies to the [password details](#) panel on the Challenge tab and to the [automatic logon](#) panel described above. If you click Yes on this option the passwords will no longer be masked: you will

be able to read them when you see or edit them. This is not especially secure but is provided for those who want as much ease as possible. Note that this does not apply to the DMH Logon mechanism, as this password can never be examined.

Safe Delete

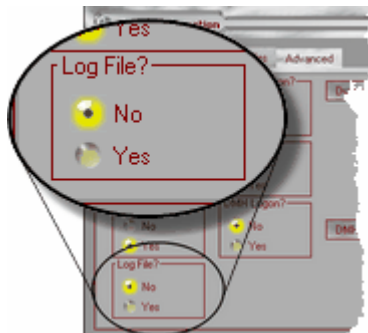
The next set of radio buttons cover the safe delete capability. DMH regards a safe boot as an attempt to get round the protection, and so by default a safe boot will trigger the delete. This behaviour can be altered by using this switch:



If the safe delete is set to 'Yes', then DMH will activate the deletion when it detects a safe boot. If it is set to 'No', then there will be no safe boot deletion. Note that this does represent a security hole.

Log File

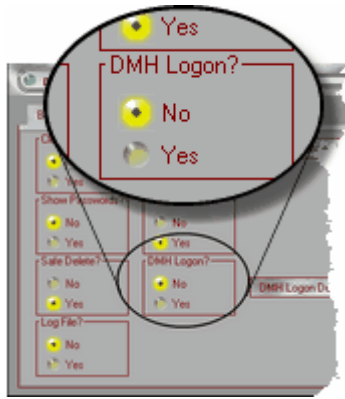
The next item is called Log File, and by default is off:



This is not for ordinary use. If it is on, then when the DMH activates it will save an encrypted log file to an arbitrary location on your hard drive. You cannot directly make use of it. If you do want to use it please contact [DMH Support](#).

DMH Logon

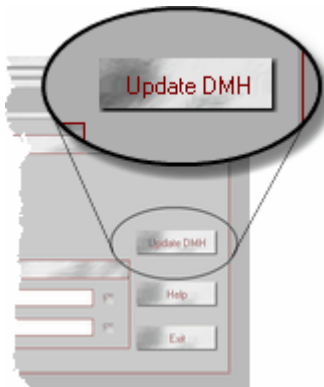
The last control is labelled DMH Logon:



This is off in the default case; it controls access to the DMH utility by allowing you to password-protect it. If you select Yes on this option the DMH Logon Details panel opens:



As in the other password requesters, simply enter the password twice. Note that in this case a blank password is not allowed. Also, this password is always masked: you cannot see it (for technical and security reasons). After having entered the password twice you will note that the status boxes are still off. Press the Update DMH button, which appeared when you selected Yes on the DMH Logon requester:



This will update DMH and the status check boxes will be ticked.

If you leave one or both of the password fields blank you will get the "Please input the password twice" message:



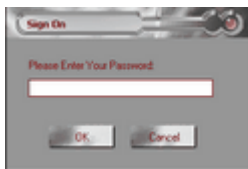
Or, if you put the password in twice but the two fields do not match you will get the "The two versions of the password do not match" message:



In both cases simply hit the OK button to clear the message and try again.

Note that if you exit the DMH utility and then return to it the two password fields will be empty in this panel. For security and technical reasons no information can be divulged about this password. You can tell if a password has been set because the status check boxes will be ticked. Note: if you turn off the DMH Logon the password is completely scrubbed - you will have to input a new password if you want to have to sign on to the DMH again.

The next time you start DMH you will be presented with the following requester:



This states: "Please Enter Your Password:". Simply enter the password and press OK. If the password matches, the DMH [basic page](#) will come up. If you press Cancel, DMH will exit immediately. If you get the password wrong, you will see:



This states "Bad password" When you press the OK button, DMH will then exit immediately.

Important: do not forget this password! If you do you will not have access to the DMH utility - the password is not recoverable. If you get this problem, please check the appropriate utility in the Tools pack (available to full licence owners).

Help and Exit Buttons

The last pair of items on this page are the standard Help and Exit buttons, in their normal location:



Help gets you to this file (or its electronic version if you are reading the paper manual) and Exit simply exits you from the DMH - no need to confirm. Should you have changed something and not updated it, you will get an [exit message](#).

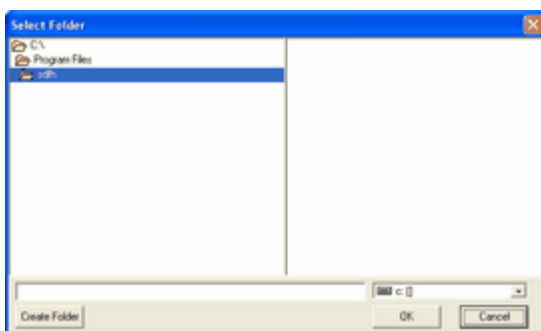
The next section describes the [Select Folder](#) window, which lets you select the main deletion folder from the [Basic tab](#) or during the [installation](#) process.

3.6 Select Folder

When you press the Select Folder button on the [Basic tab](#), the following window will come up:



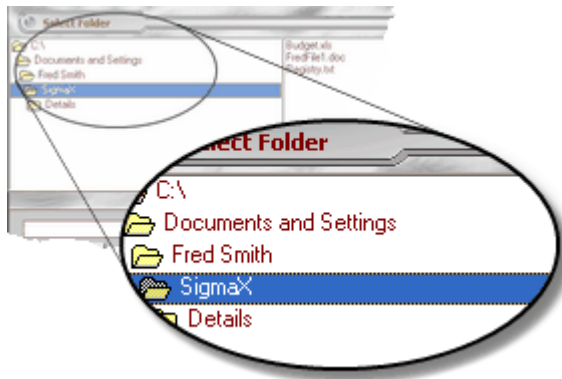
If you are using the Light version (or are in the middle of the installation) the window will look like this:



Both windows have the identical functionality, as described below.

Folder Selection

This window allows you to select folders. You navigate folders by single-clicking in the left-hand pane; the right-hand pane shows the files in the folder and is only for information purposes. There are two ways to select a folder. Firstly, you can highlight a folder by single-clicking it in the left hand pane:



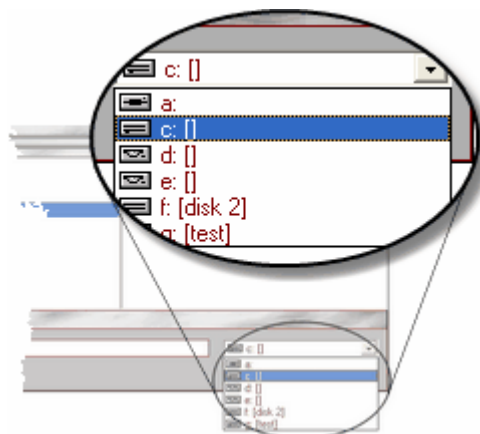
Then you hit the OK button:



On the other hand, you can also simply select the folder by double-clicking on it in the left-hand pane. In both cases you will be returned to the [Basic tab](#) or the [installation](#) with your folder selected.

Drive Selection

If you want to change drives simply press on the down-arrow button on the right of the drive selector, just above the OK and Cancel buttons. A drop-down selector will appear:



Should you select a drive that has no disk in it (such as the A: drive or a CD-ROM drive) you will

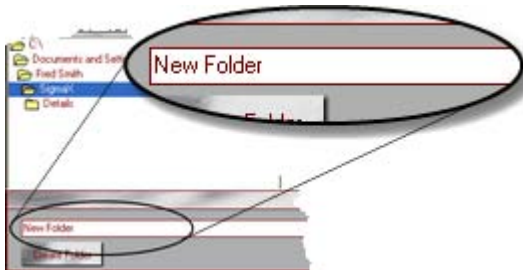
get the following error message:



The message states "Drive is not accessible - does it require a disk?". However, this should be regarded as a warning: the DMH should not be set up to try to delete information on removable drives. Similarly, the DMH should not point to network drives: they will not be available when you are off-site.

Folder Creation

You can also create a folder with this screen, and any folder you create is automatically selected as the current folder. You simply navigate to the parent folder and then type in the new folder name into the field at the lower-left of the screen:



You then press the Create Folder button:



If the folder cannot be created (usually because of illegal characters) you will get the following message:



The message states: "Failed to create folder! Possibly illegal characters were entered" This could happen if you tried to create a folder with the name "abc\def" - DMH cannot handle the attempt to create multiple nested folders. Another possibility is if you try to use special characters in folder names (for example, "." for a folder name will give an error). Lastly, this error may occur if for some reason you do not have access to the disk or folder in which you are trying to create the new folder.

If the command succeeds you will find the folder is created and opened in the Select Folder screen. Simply hit the OK button to return to the [Basic tab](#) or [installation](#) with the new folder selected.

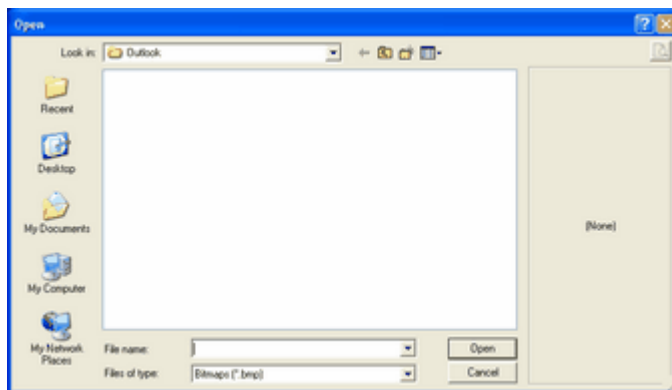
You can always exit the window without making a selection by pressing the Cancel button:



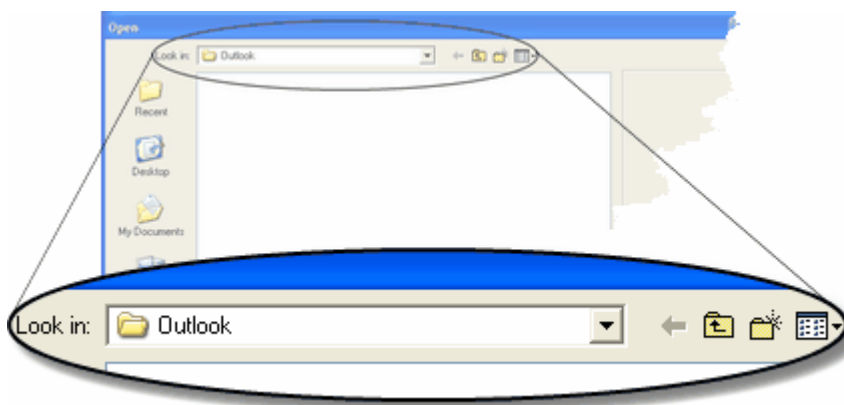
The next section describes the [Select Screen](#) window, which lets you select the main challenge screen from the [Challenge tab](#).

3.7 Select Screen

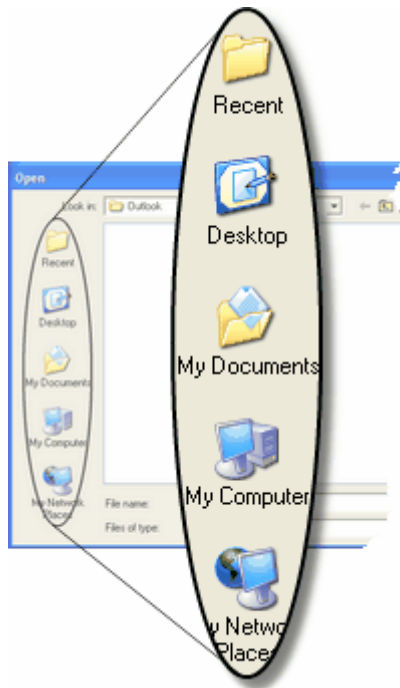
When you press the Select Screen button on the [Challenge tab](#) you will be presented with a Windows file requester designed for graphics files, which looks like this:



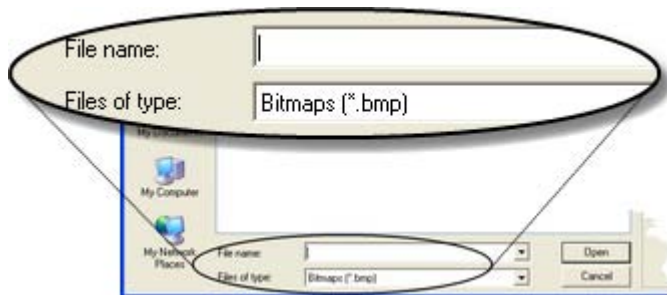
The above picture shows the requester under Windows XP; it may vary slightly depending on the operating system that you are running. Use this window as you would any normal Windows requester. The controls at the top allow you to activate a drop-down list to navigate the folder tree, go back a folder, go up a folder, create a folder and specify how you can view the files:



The panel at the left allows you to move quickly to certain "favourite" folders (this panel is missing in operating systems such as Windows 98):



Note that items such as "My Network Places" are unlikely to be useful in the context of the DMH (unless you are using the program for very special purposes). Along the bottom are the File Name and File of Type fields:

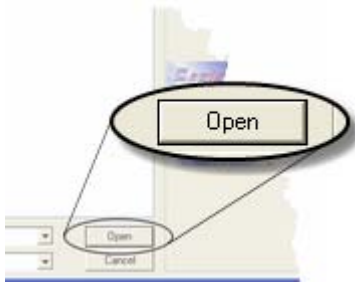


DMH generally supports Windows bitmaps (it does support other types but please see the [discussion](#) for details). You can select what files you wish to see from the lower File of Type field. Lastly, the right-hand panel will show a thumbnail of any selected graphic, as so:



Simply use this window as you would any normal Windows requester, using the top controls to move around your folders. The folders and files will be displayed in the large central window; double-clicking on a folder will open it. You can select your required file in two ways: either by double-clicking it in the main window, or by single-clicking it so it is highlighted and then pressing

the Open button:



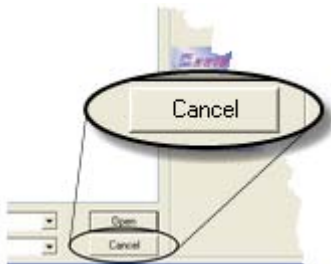
In both cases you will be returned to the [Challenge tab](#), with your selected file displayed. The file will actually be copied to the DMH home folder but you will always be shown the original location of the file (even if you subsequently delete it).

If you try to double-click or Open a file which is not a graphics file you will get the following message:



The message simply states: "That is not a valid graphics file". Press the OK button to clear it and try again.

Lastly, you can always exit the window without making a selection by pressing the Cancel button:

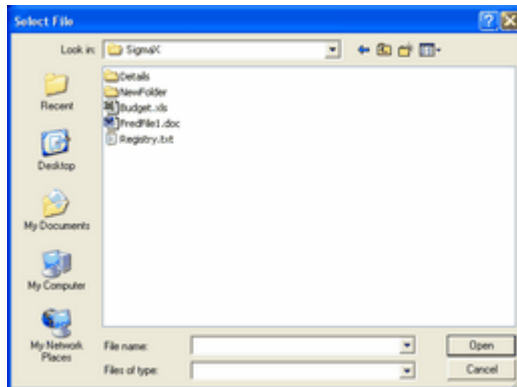


You will keep your previous challenge screen selection.

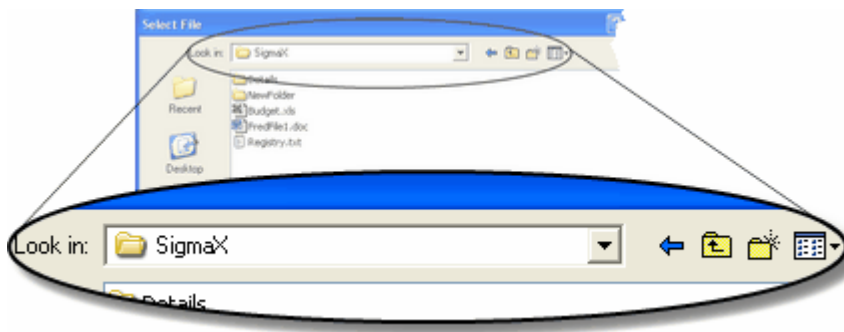
The next section describes the [Select File](#) window, which lets you add files to the [Extra Files tab](#).

3.8 Select File

When you press the Select File button on the [Extra Files tab](#) you will be presented with a Windows file requester designed for graphics files, which looks like this:



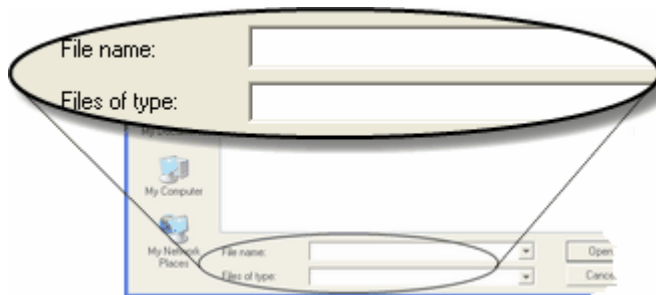
The above picture shows the requester under Windows XP; it may vary slightly depending on the operating system that you are running. Use this window as you would any normal Windows requester. The controls at the top allow you to activate a drop-down list to navigate the folder tree, go back a folder, go up a folder, create a folder and specify how you can view the files:



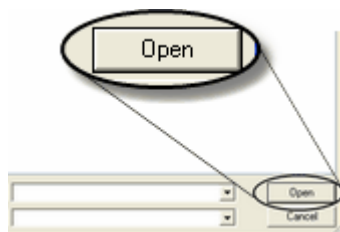
The panel at the left allows you to quickly move to certain "favourite" folders (this panel is missing in operating systems such as Windows 98):



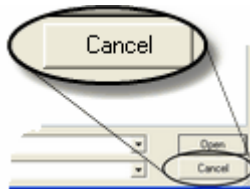
Note that items such as "My Network Places" are unlikely to be useful in the context of the DMH (unless you are using the program for very special purposes). Along the bottom are the File name and File of type fields:



You can select what sort of files you wish to see from the lower File of type field. Simply use this window as you would any normal Windows requester, using the top controls to move around your folders. The folders and files will be displayed in the large central window; double-clicking on a folder will open it. You can select your required file in two ways: either by double-clicking it in the main window, or by single-clicking it so it is highlighted and then pressing the Open button:



In both cases you will be returned to the [Extra Files tab](#), with your selected file added to the displayed list. Lastly, you can always exit the screen without making a selection by pressing the Cancel button:



In this case, no file will be added to the [Extra Files tab](#) list.

3.9 Exit Messages

As described in the [background](#) section, editing certain entries (the keycode or text fields) in the configuration utility require the use of the appropriate update button to tell DMH to update its database. Should you alter one of these fields and forget to update it you will get a message like this when you try to exit:



In the example above, the message states "You have changed the challenge keycode, but not updated it. Press OK to return and check, or Ignore and lose changes. We recommend you go back and check!". If you have changed more than one field then there will be the appropriate number of messages. We recommend that you check so you can be sure that the data in the database matches what you believe it to be. A mistake in the challenge keycode, for example, could lead to the triggering of DMH. Simply press the OK button and you will be returned to the configuration utility, whilst Ignore will just exit.

Part

4

4 Activation

4.1 Boot up and Log On

Boot Processing

When you start your machine, Windows goes through a boot process. However, there are important differences between the Windows 95/98/Me family and the Windows NT/2000/XP/2003 family. From the point of view of DMH, the main issue is security. In Windows 95/98/Me security is very weak, whereas in Windows NT/2000/XP/2003 security has been strengthened. In practical terms, you must generally log on to Windows NT/2000/XP/2003 before you can use the system, whereas on the other versions the logon is little more than a formality.

This means that in the Windows 95/98/Me systems you will always see the [challenge screen](#), as you can cancel through the logon. If the challenge is failed DMH will be activated and the [deletion process](#) will take place. With the Windows NT/2000/XP/2003 series of systems the position is not so simple. It is not possible to present the challenge before log on (under normal conditions).

Thus, for these systems you have a choice of two approaches:

1. The default approach is that the challenge is presented when somebody signs on. In this scenario the assumption is that the person in possession of the notebook has reset the Administrator's password - something that is relatively easy to do with access to the machine and software that is available on the Internet. This person will then sign on with the new Administrator's password and will promptly be presented with the challenge. The first logon after boot will always activate the challenge, irrespective of which account is chosen.

This would probably be regarded as the most secure option but does make the assumption that the attacker has some level of sophistication. Note that one of our documents on our [web site](#) discusses this further.

2. The second approach is that you want the challenge presented whenever the machine is turned on. In this case, for XP, W2000 and W2003 machines, you enable the [dummy logon](#) option and ensure that there is a dummy account set up on your machine. This should be a limited local user account, enhancing security. You tell DMH the details of this account and from then on the machine will automatically sign into this account when it is turned on. This will in turn cause the system to present the challenge screen. If the challenge is passed the system automatically logs off again, leaving you with the ordinary logon screen. If the challenge is failed the system goes into full [delete mode](#).

This option would usually be regarded as slightly less secure, in that the system goes through an automatic logon. However, DMH does then present the challenge and so can activate the deletion function more easily: the machine is acting as a trap. Note that your normal account may run at a higher privilege than the dummy account, so the dummy account mechanism may actually represent a more secure option. It is a matter of personal choice which is your preferred set up.

Note that this option is not available on NT systems: they handle automatic logons in a different way. In addition, Windows XP, 2000 and 2003 have a special capability: DMH is still active in safe boot mode, and continues to protect your machine.

Dummy Logon

We refer to the autologon account as a "dummy logon": this is because we strongly recommend that the account you use to present the challenge be separate from your normal day to day account. This account can be relatively limited and so presents less of a security threat. You could use your own account (which means the system will sign onto your account, present the challenge and then log off), but we do not especially recommend it.

One point to note is that if you do have a dummy logon set up, you can over-ride the automatic

logon by pressing the Shift key while you restart Windows. This will let you log on in the usual way (and you will still see the challenge).

As with all accounts, when you first sign on Windows usually posts all sorts of welcome messages, offers guided tours and displays information. It is a good idea to clear all this off before setting up the dummy account in DMH.

Usage

Note that for the automatic logon feature to work, the following must be true:

1. The entered user name must match that of the account.
2. The entered password must not be blank and must match the password of the account.

If you do decide to activate the [dummy logon](#) feature, be aware that other programs can also activate this feature. A very common program that does this is TweakUI, one the Microsoft Powertoys. It is important to be aware that the two systems can conflict (DMH and TweakUI), and confusion can result if you try to manage automatic logon with both utilities. Use either DMH or TweakUI to manage the automatic logon. It is the logon itself that causes the challenge, so it is perfectly valid to use TweakUI to turn this feature on if you so wish. Note that:

1. DMH may not accurately reflect the status of the automatic logon (as it maintains its own database of status information) if TweakUI is used.
2. In general, if you do use both the status of the automatic logon will be governed by the information you entered in the last utility you used.

Security of Automatic Logon

There is a potential security weakness in the use of the dummy, or automatic logon, feature that needs further discussion. DMH has to store the password to this account in plain text in a specific key in the Registry. Thus this represents a theoretical point of attack (although if the attacker is reading your Registry then DMH will have already run and the consequences of the attack will have already been dealt with). Under NT, this is also true for TweakUI. However, for Windows 2000 and XP TweakUI uses a different (undocumented) mechanism that conceals the automatic logon password. For these systems you may wish to use TweakUI to set up the automatic logon.

Failure of Automatic Logon

The automatic logon feature may not work on some systems. This will almost certainly be due to some configuration conflict. Here is a list of possible causes:

1. The special registry key DontDisplayUserName must be disabled (ie it must not equal 1).
2. If legal notice captions or text display have been enabled during logon then this will interfere with the automatic logon mechanism.
3. There is no information in the DefaultDomainName field.
4. The password entered in DMH does not match the dummy account password (note that the DMH configuration utility does NOT alter the dummy account password).

In most cases you should contact your system administrator, as these settings will often reflect your corporate policies.

Autologoff

There is now an Autologoff switch under the Advanced tab, and this will only operate when the Dummy logon is active. The purpose of this switch is to allow DMH to operate with other security software such as tracking software, whilst maintaining maximum security. If Dummy logon is set up, then the DMH will always present the challenge before the Windows logon. If the person passes the challenge, then he or she is always signed off so that they can go through the Windows password screen (for security).

If the person fails the challenge, then the Autologoff switch is checked. If it is set to 'Yes', then the person will be logged off when they fail the challenge. This represents the normal security - they have to face the Windows logon. However, if the Autologoff is set to 'No', then they will be left in

the dummy account (which should be one with few privileges). This is the situation that is preferred if the notebook has tracking software on board: the attacker can now use the machine and hopefully get onto the Internet, where they will be traced by the tracking software.

Note the dummy account will be retained if Autologoff is set to 'No' - on subsequent boots the attacker will be signed into the account automatically.

4.2 Challenge Screens

Types of Screens

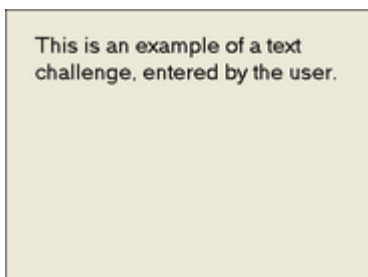
The challenge screen is the requester that appears on boot up or login, depending on your operating system (please see [boot discussion](#) for more on this). The challenge screens come in four different types based on two choices you can make, which can be found on the [Challenge tab](#). The aim is to try to make sure that you have a good selection of different screens: this means that the challenge will differ across most systems, and thus an attacker will be less likely to recognise the DMH challenge. Registered users have access to the Add-ons pack, providing a large selection of screens.

The first choice you can make governs the type of requester:

1. You may select a [graphical](#) challenge screen. In this case you may select from any number of predefined images, which have predefined text on them. You can also make your own and then tell DMH about them. Graphical challenge screens typically look this (note the space towards the bottom for the challenge mechanism):



2. Text challenge screens let you input your own text which is presented at the next challenge. It saves you the effort of creating your own graphical screens. Ignoring the challenge mechanism, such a screen might look this:



Note that the text will automatically adjust in size according to the amount that is entered. The system can handle up to 600 characters for the text.

The second choice you have is the way that you are challenged. Basically, there are two mechanisms:

1. The first is based on a [key code](#). This is where you are presented with a grid of 16 buttons, a combination of which you have predefined to be the key code. This is the recommended way to set up the challenge, as it is relatively easy to set up a memorable pattern. In addition any number of the buttons may be used, from none to all sixteen. Note that the key code must be entered correctly and the OK button pressed for the challenge to be passed. An incorrect key code, or pressing the Cancel button, will cause the DMH to activate. As an example, this is what the first screen above looks like with the challenge mechanism displayed:



2. The second is based on a [password](#). This is where you are presented with a password challenge, which you have predefined on the [Challenge tab](#) of the DMH utility. Passwords of any length may be used but it should be noted that there is a greater risk of getting the password wrong - and activating the DMH. You can also have passwords of 0 length: in this case the DMH will be activated if Cancel is pressed but not if OK is pressed. This is the way the first screen looks with a password challenge:



Naturally, either the key code or password mechanism may be used with the text challenge system.

Making Your Own Challenge Screens

DMH comes with a large number of challenge screens in the Add-ons pack, any of which you may use. You will also find more screens on the [DMH support website](#), all of which may be freely downloaded and used. However, you may wish to provide your own. In this case, the following are the rules for DMH screens:

1. All screens are 400 pixels wide by 300 pixels high. Any other size will look odd as the graphics will be either too small or too large.
2. The preferred format is Windows bitmap (typically, files with a .bmp extension). Any type of bitmap will do (ie 256 colour, 16 bit colour, 24 bit colour and so forth). DMH will support Windows metafiles (either of type .emf or .wmf) but the benefit of smaller file sizes will only be gained under special conditions.
3. You should match the quality of the bitmap to the bitmap's contents. Plain colours can use 256 colour (or even fewer) bitmaps; photos will require high-quality 16 bit or higher bitmaps. This will have an impact on file sizes.
4. Having created your bitmap, simply tell DMH where it is on the [Challenge tab](#) of the DMH utility. The file will be copied to the DMH installation folder. You can if you wish remove the original from your disk (although DMH will "remember" where the original came from).

You may use any graphics editor to produce such screens. This mechanism allows "badging" of your system and the use of custom screens reduces the likelihood of DMH being recognized by the

attacker.

Prompt on Challenge

If you fail the challenge, either by inputting an incorrect password/key code or by hitting the cancel button, by default DMH is configured to go immediately into deletion mode. This may be regarded as somewhat Draconian, so the capability is provided so that you can give yourself extra chances by selection of the [appropriate option](#) on the Basic tab. This will allow you to choose the number of attempts you would like to have, and what you would like displayed.

You can just having something shown to you if you are actually failing the challenge (the fail prompt). You could possibly use this to give yourself a clue as to what your password or keycode is. You can also have a different message shown if you are passing the challenge: this has been offered so that even if the attacker has some idea of what they are doing, they do not know if they are currently passing or failing the challenge.

When you are prompted, if you press No you will be returned to the challenge screen. If you press either Yes or the cancel button (the "X" in the top right) DMH will continue. Note that if this meant passing the challenge then DMH will pass. If you were about to fail the challenge, then on hitting Yes DMH will continue and delete the appointed files and folders. Also, if you exceed the number of tries then DMH will go into delete mode: even if you are currently passing the challenge.

We do not particularly recommend the use of this prompting system: it increases the likelihood of the attacker guessing that DMH is on the system. However, whilst you are getting used to the system it may be worthwhile using this to reduce the possibility of an unwanted file deletion.

4.3 Deletion Approach

DMH tries to remove as much information from your system as possible. It tries to ensure that no clues are left behind (such as sensible deleted file names). The system has the following approach when it is activated. It is driven by your [security settings](#) but the sequence of events is approximately as follows:

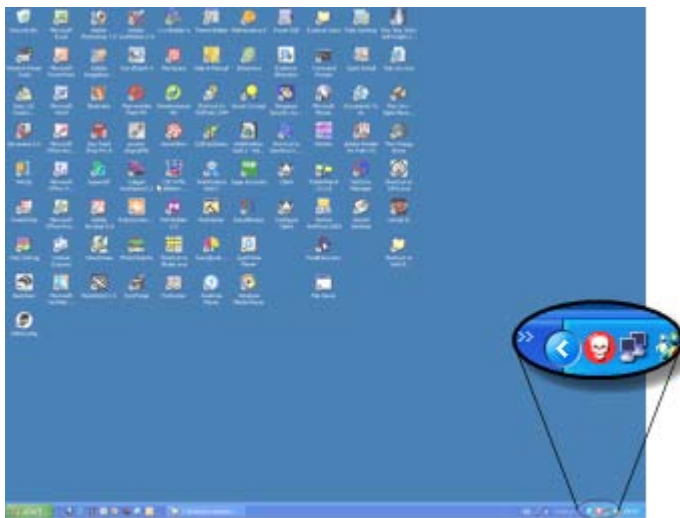
1. When the challenge is presented, the system will look normal. However all the desktop icons, the Start button and the task bar will be unresponsive. Ctrl-Alt-Del and similar key combinations will be ignored.
2. Entering a wrong password or keycode and pressing OK will fail the challenge. Pressing Cancel will also fail the challenge.
3. Once the challenge has been failed DMH immediately activates. It maintains the disabling of the desktop, Start button and taskbar. It tries to ensure that the following sequence will not be interrupted.
4. DMH then works through the security folder, getting each file in turn. It starts on the lowest level folders first.
5. Each file is overwritten according to the [security settings](#). The overwrite always increases the file size, to wipe out all possible slack space in the file. Note that the Minimal setting, which does not overwrite, skips this and the next three steps.
6. Each file is then renamed according to a random algorithm.
7. Each file is then truncated to 0 length.
8. Each file then has its time stamps randomized.
9. Each file is then deleted.
10. As the folders are emptied, they are then also renamed, have their time stamps modified (not Windows 95/98/Me) and are deleted.
11. Having worked through the security folder DMH then deletes the extra files in turn, following the process outlined in steps 4 to 7.
12. If required, it will try to remove any disk [transaction logs](#) that may exist.
13. Having completed the extra files, DMH then deletes itself. It tries to clear down all its own files, its registry settings and any temporary files and folders.
14. The last thing it does is release the assorted locks, and then spawns out to a tidy-up batch file.

There are some things to be aware of:

1. The process will usually work as indicated. However, if you activate the DMH via the [panic button](#) some files that you have nominated for deletion may be locked (you may, for example, be working with them). See the [discussion](#) on this point.
2. In general, if DMH cannot delete a file then it will fail gracefully and abandon the attempt in the worst case. It will carry on with the other files.
3. Some features are dependent on the operating system. For example, folder timestamps are much less exact under the Windows 95/98/Me systems than under the NT/2000/XP/2003 series (and there are differences between the operating systems in the details in how time stamps are handled).

4.4 Panic Button

As a default, the panic button is enabled. This capability allows you to interactively fire off DMH, should you feel a need to do so. When the option is enabled a small red and black icon is placed in your system tray in the lower-right hand corner of your screen:



You may have to open up the system tray to see it. Clicking the icon calls up the panic button in the middle of your screen:



You may now do one of three things:

1. Left-click on the red button: this will activate DMH in the same way the [challenge screen](#) does if a person fails a challenge on [bootup](#).
2. Left-click on the Cancel button: this will return the panic button to the system tray.
3. Right-click anywhere over the two buttons. This will give you the menu option Exit. Clicking on this will disable the panic button for the rest of this session (note: it will get replaced in the system tray the next time you start the system). Use the [configuration utility](#) if you want to disable the panic button permanently.

You may be working on files marked for deletion by DMH when you hit the panic button. In this case, they will usually be locked: although DMH will attempt to delete them, it may not be able to do so (the exact state of [locking](#) depends on your software and exactly how the files were opened).

If you have enabled the [challenge prompt](#) on the Basic tab, then the following screen will be displayed when you press on the red button:



This asks if you are sure. If you press No you will be returned to the panic button. If you press Yes or Cancel (the "X" in the top right) DMH will continue to delete the files. Note that the panic button does not use the self-specified prompts as they are not especially appropriate for the panic button.

We do not especially recommend the use of this check: it delays the application of the panic button.

If in your current computer session you have disabled the panic button by using the configuration utility, you will not notice any apparent change: the icon will still be in the system tray. However, if you try to use the panic button it will just exit without deleting the files.

The panic button has feedback "rollover" effects on Windows 2000, 2003 and XP operating systems; these are not available on the other Windows systems.

Part

5

5 Useful Information

5.1 Extra File Information

The following discussion is to help you decide what extra files should be included as high security files that ought to be deleted if your notebook is stolen. We also try to give some information about where to find these files. Some other file considerations are also covered.

Mail Files

If you have a local mail file on your notebook this will almost always have information in it that you would rather not have openly read. Mails frequently discuss items that are in your Confidential class of information. We would always recommend that your mail file is included, especially as frequently this file also has your contacts database (this is the case if you are using Microsoft Outlook). You have an obligation to your contacts to keep their details secure.

However, finding your mail file can be less than straightforward. This is because different suppliers take different approaches and even change their minds from one version of their mail system to the next. In addition, the path names tend to be long and, at least in some cases, fairly grotesque. At the time of writing, here are some tips to help you find your mail files:

1. Outlook. If you are using Exchange Server then see your System Administrator. Otherwise, you will almost certainly be using POP3 for mail. In this case Outlook puts everything into one file (mail, calendar, contacts, etc), which always has a ".pst" extension and is usually called Outlook.pst. The easiest way to find it is to open up Outlook and go to the File menu. You will see an entry called "Data File Management". Click on the entry and then click on "Open Folder": this will give you the full path of the file. If you are being sophisticated in your use of Outlook, you may have more than one ".pst" file.
2. Outlook Express. This puts mail into different files; right-click on the given mail folder within Outlook Express and look at Properties. This will give you the path for that folder in "This folder is Stored in the Following File" field (which will be a ".dbx" file, as in Inbox.dbx). You can click on this field and use the cursor arrows to scroll through (so you can actually read it, as the paths are usually too long to fit). You should also be able to select the field's content and copy/paste it, if required.
3. Netscape Mail. You can quickly get the path name by right-clicking on the mail folder and selecting "Copy Folder Location". This places the complete file path on the clipboard. You will have to convert the slashes into backslashes and convert the front 11 characters to C:, but then you can paste the string into DMH.
4. Mozilla Mail. See Netscape Mail above.
5. Eudora Mail. Eudora stores its mail files in its own folder (by default C:\Program Files\Qualcomm\Eudora). Each mail folder has two files: a ".mbx" file for data and a ".toc" file for the index.

Another way to find the files is to put the extension into the Search utility under Windows, or for most mail systems look for "Inbox".

Other Files

Other files that should be considered:

1. Any contacts databases on your system (which will be separate if you are not using Microsoft Outlook).
2. Calendars and "To Do" lists.
3. Information that may be backed up from your PDA.
4. Spreadsheets.
5. Databases you have on your notebook.
6. Documents (especially if they have change tracking in force).
7. Expenses.
8. Anything containing client or supplier details.

The other important habit to get into is to keep the number of confidential files on your notebook as low as possible. Make sure they are backed up on the home server, then delete them when you

have finished with them.

File Sizes and Considerations

DMH currently has a limitation on the maximum filesize: 4GB minus 2 bytes. However, be warned that files of this size will take a long time to delete. It is strongly recommended that your secure files be as small as possible, subject to the following.

There is another issue with regard to file sizes: later versions of NTFS and small files. If your file is smaller than around 800 bytes, then NTFS will store the file data within the disk's master file table. The effect of this is to have the file data appearing in the system log file. DMH could attempt to clear the log file in this case, but because of its size this can take a long time. So for the present this feature has not been implemented.

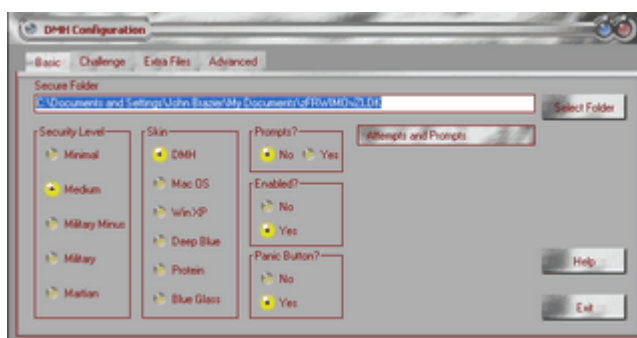
Thus the rule of thumb is make sure that the files you protect are greater than 1KB. This should not be a problem: the following is a list of minimum file sizes from a number of different products (as shown by Windows, to the nearest 1KB, values may vary according to version):

| | | |
|----------------------|-------|-------|
| Adobe Acrobat | 14KB | |
| Adobe Illustrator | | 157KB |
| Adobe Photoshop | 7KB | |
| Microsoft Access | 100KB | |
| Microsoft Excel | 14KB | |
| Microsoft Powerpoint | 8KB | |
| Microsoft Project | 111KB | |
| Microsoft Word | 24KB | |
| Microsoft Visio | 16KB | |
| Paint Shop Pro | 2KB | |
| Wolfram Mathematica | 3KB | |

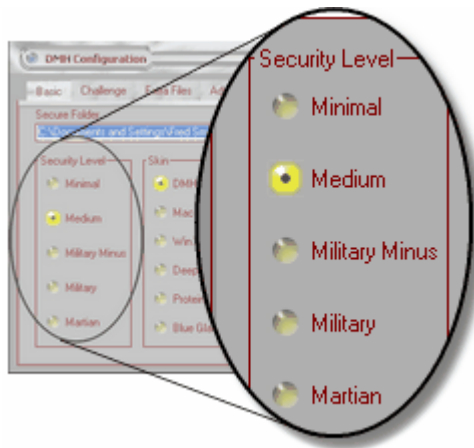
'Minimum file size' means saving as small or empty an object as possible from the application. Note that it is invidious to compare file sizes: some applications require much more set up than others. The key point is that most modern software always produces file sizes larger than the 800 bytes that will not be stored in the master file table.

5.2 Security Levels

When you start up DMH you will see the basic page, on the [Basic tab](#):



There are five levels of security, indicated in the left-hand column of the screen:



These levels govern how thoroughly DMH will wipe your files. This section discusses how the deletion mechanisms differ and makes some recommendations.

Minimal

The Minimal security setting is just that: when DMH is activated, it simply deletes the files using the operating system's normal file deletion system. The files are not overwritten, their time stamps are not altered and they are not renamed. This does little more than hide the files, as they will be recoverable with any decent file recovery utility, and they will still be in their hierarchical folder structure. The only benefit is that this deletion process is fast. The security provided is, well, minimal.

Medium

When DMH is activated at the Medium security level, it does the following:

1. Overwrites the file with one pass of random numbers. It extends the file size to overwrite all slack space.
2. Renames the file with a random name and extension.
3. Truncates the file to 0 length.
4. Randomizes the file's time stamps.
5. Actually deletes the file.

This gives a much higher security protection. The files have been overwritten and all audit information removed. File recovery utilities will have problems because of the file truncation: all the file blocks have been deallocated, and are no longer associated with the now meaningless file name. Even if any content can be recovered, it has been overwritten with random numbers produced by a strong pseudo random number generator (PRNG). It should be noted that some of the older operating systems, such as Windows 95 or 98, interfere with the file renaming process but attempts are made to circumvent this problem (even if 100% success cannot be guaranteed).

This is the generally recommended setting for normal security. It also works well with file encryption. It is the best compromise between security and speed: DMH still operates rapidly at this security setting.

However, if you have concerns there is the next level of security.

Military Minus

This is a level of security defined by the Department of Defence DOD Standard 5220.22-M, otherwise known as the "NISPOM" (National Industrial Security Program Operating Manual). During the deletion process it specifies the following steps:

1. Overwrite all locations with a character.
2. Overwrite all locations with the character's complement.
3. Overwrite all locations with a random character.
4. Verify the last write.

At this level of security, DMH does the first three steps during the deletion phase. It then continues with the file renaming, truncation and so forth. The one thing it does not do is the final verify of the random number write, for two reasons: (a) speed; and (b) there is little that can be done if the overwrite has failed.

This level of security pragmatically matches the DOD standard. It should be noted that the character and its complement used in the writes are not 0 and 255, but a character and its complement that maximally produce strong fields over as many disk types as possible, to improve the deletion. This level of security significantly slows down DMH.

Military

This is the same as the Military Minus level, except that the verify is carried out. The sole purpose is to provide the capability of full DOD standard deletion to any person who requires it. Note that DMH will not actually report a verify failure except via the hidden and encrypted [log file](#), which is of little use as it cannot be accessed (presumably).

Martian

This is the highest security level possible and is based on P Gutmann's paper *Secure Deletion of Data From Magnetic and Solid-State Memory*, presented at the Sixth USENIX Security Symposium in 1996. This level has been specified as it has acquired a certain cachet in the computing community.

Gutmann's procedure describes the following deletion process:

1. Four overwrite passes with random numbers.
2. 27 overwrite passes of specific bit patterns.
3. Four passes with random numbers.

The middle 27 passes are randomized so that the bit patterns are not put down in the same order from file to file. The patterns are specially defined to produce maximum magnetic fields over the disk surface so that the erasure of previous data is optimally efficient. There are a number of different patterns to cater for the different encodings that different models of disks have used during their development over the last 30-plus years. The objective is to ensure that no trace of the original data exists, even if the most advanced surface-probing technologies are used.

Of course, the procedure is trying to cater for lots of different drives, so for any given drive there is a large overkill in terms of file wipes. In addition, modern drive encoding mechanisms undermine some of the aims of this wiping process. However, with 8 overwrites of random numbers along with 27 runs of assorted bit patterns, you can be pretty sure that the information in the target file is as destroyed as it will ever be with an overwriting process.

Thus it is difficult to recommend this security level unless the information is extremely sensitive: it really is overkill. If you do use this level the files should be small and few in number, otherwise the process will take some time.

Discussion

The five levels of security increase in protection whilst they decrease in speed. The optimum is a compromise. We recommend the Medium setting unless you have good reasons for choosing another setting. The reasons for this are:

1. DMH is still fast when overwriting with just one pass.
2. It is most unlikely that any normal attacker can recover information from a disk after only a single write. Techniques for such recovery do exist but it is noticeable that no data recovery company offers a data recovery service after the file is known to be overwritten. The technology to examine the track edges to recover the old bits is slow, labour-intensive, expensive and still problematic.
3. A single write is compatible with the use of encrypted files (which might already be securing your data) and will also work with compressed drives (even though we do not recommend the use of drive compression with DMH). There is no point in using the Gutmann procedure with compressed drives (and some modern drives) as the patterns will be altered by the compression/encoding process.

4. Much of the DMH functionality comes from its "scrubbing" of the audit trail: renaming files, changing timestamps and removal of their size information. This makes the recovery process much harder, even with a single overwrite.

If you do feel that one single overwrite is not enough, then go for Military Minus. This effectively gives three overwrites and will make any recovery of data extremely problematic.

Ultimately, if the person who has stolen your notebook has very large resources they will be able to access your information whatever you do. This will, however, be via subversion of employees rather than analysis of notebook contents.

It should be remembered that the aim of DMH is to protect your information from loss of notebooks, where the attacker can be expected have either limited computer knowledge or limited resources. DMH is not designed to protect your information from government-class hostiles.

5.3 Installation Defaults

When you first install DMH it comes with default settings. These are now described.

Basic Tab

| | |
|----------------------|--|
| Secure Folder: | Points to a folder under your "My Documents" folder, which may be called "<Your Name's> Documents" on the Windows 2000, 2003 and XP operating systems. |
| Security Level: | Medium. |
| Prompts? Enabled? | No. Yes. |
| Panic Button? | Yes. |
| Skin: | DMH. |

Challenge Tab

| | |
|---------------------------------|--|
| Challenge Screen: Requester? | Points to the file "b.bmp", and is a copy of the "Zalgot" file. Graphics. |
| Text of Challenge: | Hidden - but set to "???". |
| Challenge Type? | Key Code. |
| Key Code Details: | The 3 will be ticked. |
| Password Details: | Hidden - but set to "abc". |

Extra Files

| | |
|--------------|-------------------------|
| Extra Files: | The list will be blank. |
|--------------|-------------------------|

Advanced Tab

| | |
|------------------|--------------------|
| Clear Page File? | Yes (if visible). |
| Dummy Logon? | No (if visible). |
| Show Passwords? | No. |
| Autologoff? | No (and disabled). |
| Safe Delete? | Yes. |
| DMH Logon? | No. |
| Log File? | No. |

5.4 Passwords

There are three different passwords understood by DMH; it is worth describing the three to ensure that their usage is clear.

Challenge Password

This is the password that you must put in when the system [boots up](#). This password may actually be a [key code](#) challenge or a [password](#) challenge. This is the core password of the DMH system: it is the one that when the attacker fails will launch DMH into its deletion mode. There are a few things to note about this password:

1. It is case sensitive! Always make sure that you know the state of the keyboard when you enter the password.
2. It may be as long or as short as you like. Normal password considerations do not apply here: a "dictionary" attack is not possible (one failure and DMH is launched). Make sure it is a password that you will not get wrong.
3. You can actually have no characters at all for the password. In this case, the challenge screen becomes a 50/50 chance whether or not the attacker fires DMH. If the attacker hits OK DMH will back down; if the attacker hits Cancel then DMH will launch into delete mode.
4. If you select [show passwords](#) from the [Advanced tab](#) you will be able to see this password in plain text when you enter it into the DMH [configuration screen](#). Note that the password is actually stored in an encrypted form and is masked when the [challenge screen](#) is displayed.

Dummy Logon Password

This is the password that the system uses during [boot up](#) to sign on to the dummy account (for 2000, 2003 and XP systems). Windows uses this password to automatically go into the account, so that the [challenge screen](#) is displayed. This password is actually stored in plain text in the registry (by Windows), so you can also see this password in plain when entering it in the DMH [configuration screen](#) by selecting [show passwords](#) in the [Advanced tab](#). Remember - you can also use [TweakUI](#) to maintain this password.

DMH Logon Password

This password is quite different from the other two: it protects access to the DMH configuration utility itself. You will have to enter it every time you start up DMH and it is case-sensitive. Because this password is stored in a hashed format, and because it controls access to the DMH configuration screens, [show passwords](#) has no effect on this password when you turn it on in the [configuration screen](#): the password is always masked. If you forget this password when this feature is active you will not be able to use the DMH configuration utility: check out the Add-ons pack for help.

5.5 Random Number Files

DeadMan's Handle uses its own random number generator. The state of this generator is maintained in a file called SF.bin, which is constantly being updated. DMH ships with a default SF.bin, which naturally is the same for all people who purchase the product. This can lead to a potential concern that many machines may have their random number machine in approximately the same state, potentially compromising security.

To counter this concern, the purchased version of DMH is shipped with 1000 random number generator state files. These are available on the CD or in the downloaded package: see the README file for the location. Any of these files may be selected and copied to the installation folder, as long as the selected file is renamed to SF.bin. This will then reset the random number generator to another state.

At regular intervals we will be providing new state files, as a service to our customers.

If you wish, you can generate your own file. The format is straightforward: the first 1024 bytes are completely random binary numbers. The rest of the 4KB file is padded with 0 value bytes: the file

must be a full 4KB bytes long. The 3KB of 0 byte padding is reserved for future development.

5.6 Usage Information

Locked Files

DMH will try to delete all files that it has been instructed to delete. In effect this means all files and folders in the Secure Folder plus the specially chosen extra files. Above the Minimal security level DMH will also attempt to overwrite, rename and truncate the files, and scramble the file dates.

In all cases DMH will try to carry out these actions even if the file is locked. This would only ever happen in the case that DMH was activated via the [panic button](#): if DMH is activated via the [bootup](#) challenge screen then no files should ever be locked (unless you are trying to delete a system folder).

However, in the case of a locked file DMH will try to delete it and then fail gracefully, continuing on to the next file or folder. This "abandoning" of the locked files can lead to different effects depending on the operating system:

1. Under the NT series, the file will lead to the folder being locked. This means that the file, folder and any parent folders will still be left behind after DMH completes.
2. Under the 9x series, a folder can still be accessed, even if it cannot be deleted, when it contains a locked file. This means that the rename function works. The folder is effectively moved, still containing the file, to under the root folder of the drive, with a random name. Note that all parent folders now get deleted as the folder with the locked file has been moved. Although under the 9x series the locked file and folder have not been deleted, they do get "lost".

One other important limitation of the Windows 9x series is that the folders do not get their time stamps altered: this is not possible under these operating systems.

Page File Cleardown

When you select the [clear page file](#) option you are actually setting a registry value. This in turn tells Windows NT/2000/XP/2003 to overwrite the page file with zeros when you shut the system down. This is done as an attempt to reduce the amount of analyzable information on the machine. However, there are a few things to be aware of:

1. Not all the page file will get wiped. Some parts of it will still end up being locked, as Windows has not shut down.
2. The wiping is a single-pass write of zeros. As discussed [elsewhere](#) information is still theoretically recoverable after a single overwrite, so this measure is not perfect.
3. Wiping the page/swap file reduces information leakage but Windows still has ways of writing out information to your hard drive (basically, unused file space gets bits of memory dumped to it; as files move around the disk, these old chunks of memory tend to stay there and accumulate unless they are specifically overwritten). To deal with this issue consider using a disk cleaning tool.
4. Wiping the page/swap file does slow down the system shutdown.

However, despite the above comments we generally recommend switching the clear page file option on if you are running DMH on an NT/2000/XP/2003 system. It reduces information exposure and makes the attacker's job harder.

Operating System Limitations

Some of the earlier operating systems have limitations that affect the performance of the DMH. In essence, a few of the DMH's capabilities are not available in earlier operating systems. Some of the limitations include:

1. Windows 95 and Windows NT cannot use a "skinnable" user interface: a special plain interface is provided.
2. "Safe boot" under Windows 2000, 2003 and XP systems will activate the deletion, to stop circumvention attempts, if required. This capability is not available under Windows 95, 98, Me

- or NT systems.
3. The dummy logon feature will only operate under Windows 2000, 2003 and XP (although the equivalent exists for all the other operating systems by not having a logon at all - but this has security implications under NT).
 4. The clear page file capability will only operate on Windows NT, 2000, 2003 and XP systems.
 5. As covered above, folder timestamps are not altered on the Win9x systems.

XP has one limitation: system restore points. If DMH is placed in a folder that is being monitored (which will be the usual default situation) then the system will monitor it. After installation, you should disable monitoring for the DMH folder (in the registry key HKLM\System\CurrentControlSet\Control\BackupRestore\FilesNotToBackup) and create a new restore point manually. Otherwise, XP will retain information about DMH even when it has deleted itself - which potentially could 'leak' information that DMH was on the machine at some time.

Security Points and DMH Self-Protection

DMH takes a number of steps to protect itself - and your data - when it is operating. When the challenge screen is displayed DMH will do the following:

1. Lock the task bar.
2. Lock the desktop.
3. Lock out special key combinations (such as Ctrl-Alt-Del).
4. Disable any Explorer windows that are open.
5. Disable any task manager windows that are open (not applicable to Windows 95, 98 and Me systems).

This is to enforce interaction with the challenge screen. The same lockouts also take place when the deletion process is triggered.

However, this does have some implications. The first is that many modern programs provide Explorer-type interfaces within their own system. If such a program is placed in the Start menu, then it will be started up automatically, alongside the DMH. This represents a point of weakness in that the criminal could investigate the system using the program and ignore the challenge screen.

DMH does make the challenge screen the active screen at regular intervals, making any such attack a great deal harder. However, we recommend that careful consideration be given to programs that are placed in the Start menu.

In a similar way, special toolbars with special capabilities also represent a possible weakness, as again they may provide an attacker to an Explorer-like interface. Again, we would recommend activation of such tools after the challenge has been passed.

General Points

Because of the way Windows works, it can take a short while for shortcuts and system tray icons to be updated. This is normal.

Most of the DMH skins assume usage of high colour or true colour on the desktop. If you are using a 256 colour display, then the light installation will look better.

An entire disk may be designated as the secure folder (such as "G:\"). If this disk contains only data, then DMH will function as expected. If, however, the system disk is so designated then there will be a problem. At some point DMH will start deleting the system area, which will ultimately lead to a crash and a corrupted system that may well not reboot. DMH will not complete, so will still be on the system, and so may be some or all of the confidential information. It is impossible to predict when DMH will start working on the system folders, as it will depend on the overall folder structure. Do not designate the system disk as the secure folder.

Part

6

6 Support

6.1 Support

Free support is always available by eMail from:

support@deadmanshandle.com

In addition, FAQs, white papers, support information and updates are available at our web site:

www.deadmanshandle.com

Lastly, support and service contracts are available to customers with guaranteed response times and formal escalation procedures. Please contact:

sales@deadmanshandle.com

6.2 Credits

Just to take the opportunity to credit all sorts of people, without whom DMH could not have existed.

Bob Jenkins for the [ISAAC PRNG](#)

Peter Gutmann for the [Secure Deletion paper](#)

Joan Daemen and Vincent Rijmen for the [AES \(once Rijndael\)](#)

Vincent Rijmen, Antoon Bosselaers and Paulo Barreto for the AES code

NIST for the [SHA-1](#)

Ross Anderson for his [Security Engineering and his many other papers](#)

Thanks to [Blue Valley Systems](#) and Eric Brough for their general help and testing.

Thanks to Nick Beech for the design work.

Thanks to Evgeny Tarasov and Ken Hayward for bug hunts.

Windows is a trademark or registered trademark of Microsoft Corporation. All other trademarks are the property of their respective owners.

Help and manual developed using Help & Manual.

Thanks to TetaSoft, Sam Solutions, Sunisoft, 7Bear and Utilmind Solutions for licensing their technology to us.

Hemera and Focus Multimedia supplied some pictures.

Space pictures courtesy of NASA, JPL-Caltech and the USGS.

Poetry courtesy of William Blake, Lewis Carroll, Christopher Isherwood, J B Morton.

Trek in Vegas Copyright Tony Walters.

The blue-footed boobies are Copyright by Tom Dempsey / Photoseek.com.

© 2004,2005 DeadMan's Handle Ltd.

Index

- A -

Advanced 29
 Autologoff 29
 Challenge Check 29
 Clear Page File 29
 Configuration 29
 DMH Logon 29
 Dummy Logon 29
 Log File 29
 Logoff 29
 Page 29
 Safe Delete 29
 Show Passwords 29
 Tab 29

- B -

Background 13
 Configurations 13
 Editing 13
 Help 13
 Screens 13
 Title Bar 13

Basic 15
 Configuration 15
 Enable/Disable 15
 Page 15
 Panic Button 15
 Secure Folder 15
 Security Levels 15
 Skins 15
 Tab 15

Boot Up 47
 Autologoff 47
 Automatic Log On 47
 Challenge 47
 Discussion 47
 Dummy Log On 47
 Issues 47
 Log On 47

- C -

Challenge 20
 Graphical 20

Key Code 20
 Page 20
 Password 20
 Screen 20
 Setup 20
 Tab 20
 Text 20

Challenge Screens 49
 Discussion 49
 Graphics 49
 Make Your Own 49
 Text 49
 Using 49
 Configuration Pages 13
 Credits 64

- D -

Dead Man's Handle 4
 Defaults 59
 Deletion Approach 51
 Deletion Discussion 51
 Deletion Process 51
 DMH 4
 DMH Defaults 59
 DMH Support 64

- E -

Exit Messages 45
 Extra File Information 55
 Considerations 55
 File Sizes 55
 Mail Files 55
 Other Files 55
 Extra Files 27
 Adding 27
 Page 27
 Removing 27
 Tab 27

- F -

File Sizes 55

- I -

Installation 7
 Information 7
 Options 7

Introduction 4
Benefits of DMH 4
DMH Features 4

- M -

Mail Files 55

- P -

Panic Button 52
Description 52
Usage 52

Passwords 60
Challenge 60
Discussion 60
DMH Logon 60
Dummy Logon 60

- S -

Security Levels 56
Discussion 56
Martian 56
Medium 56
Military 56
Military Minus 56
Minimal 56

Select File 43
Adding Files 43

Select Folder 37
Secure Folder 37

Select Screen 40
Challenge Screen 40
Graphics Files 40

Setup 9

Small Files 55

Support 64

Support for DMH 64

System Defaults 59

System Requirements 5

- T -

Three Steps 9

- U -

Usage Information 61
Deletion 61

Discussion 61
Earlier OS 61
General Points 61
Locked Files 61
Page File Cleardown 61