DESlock+
Protect your data.
www.deslock.com
DESkey
User manual

Certain features and functions of the DESlock$^+$ software and the associated hardware key are protected by patent. Patent GB2378539 refers. Worldwide patents applied for.

Software Licence

PLEASE READ THIS CAREFULLY BEFORE YOU OPEN THE CD DISK PACKAGE

YOUR RIGHT TO USE THIS PRODUCT IS SUBJECT TO THE TERMS SET OUT BELOW. BY USING THIS PRODUCT YOU ARE ACCEPTING THESE TERMS.

1. DEFINITIONS

1.1 In this Agreement the following words have the corresponding meanings:

"Agreement" this licence agreement;

"DES" Data Encryption Systems Limited (Co No. 1934623) of Silver Street House, Silver Street, Taunton, Somerset TA1 3DL England;

"Distributor" any third party authorised by DES to licence the Products to third parties on behalf of DES;

"Documentation"the user manual and any other documentation supplied as part of the Software help system;

"Information" any information or data encrypted or decrypted using the Software and/or the USB Hardware;

"IPR" all intellectual property rights in the Products (and any part of them) including without limitation the Specific Rights, any copyright, registered or unregistered trademarks, patents, database rights together with any applications to register the same anywhere in the world;

"Licence" a non-exclusive, non-transferable licence to use the Software and or the USB Hardware and Documentation in accordance with the terms of the Agreement;

"Products" the Software, the USB Hardware, and the Documentation;

"Software" the software entitled DESlock+ used for the encryption and decryption of electronic data.

"Specific Rights" the registered trademarks DESlock, DESlock+, DESkey, Patent GB2378539, US Patent Application 10/085,163, International Patent Application PCT/GB2002/003877 and European Patent Application 02751448.8.

"USB Hardware" the USB hardware device for use with the Software;

"Qualifying Personal user"
A person using the Software solely in a personal capacity for personal data this includes full and part time students who use the software with any information related to their studies and research and any correspondence with their school, college or other institution or any other organization which is involved in their personal training or education.

"Corporate Users"
Persons using the Software with information belonging to a business or any other organization of which the user is an employee or member of or is working for under any contractual or voluntary basis including working as self employed with the exception of correspondence directly relating to the single user such as personal contract of employment or correspondence relating to the terms and conditions of your employment.

1.2 All references to the plural shall include the singular and all references to the masculine shall include the feminine and neuter and vice versa.

2 GRANT OF LICENCE AND DES OBLIGATIONS

In consideration of you agreeing and adhering to the terms of this Agreement, DES grant you a Licence.

2.1 Qualifying personal users as defined in this Agreement may use the Software without the USB hardware by way of a Software key-File available free of charge from DES.

2.2 Corporate users as defined in this Agreement are NOT permitted to use the software free of charge other than for initial evaluation purposes at the express permission of DES.

3. PERMISSIONS

Subject to this Agreement you are permitted to:

3.1 load and use the software on one or more computers for your own use (in object code form only) in conjunction with the USB hardware or software key-file;

3.2 make a back-up copy of the Software in support of your permitted use of the Software provided you clearly label the back-up copy with the following notice:

© Data Encryption Systems Limited [2002] - All Rights Reserved

3.3 use the USB Hardware for the purpose of generating and storing encryption keys;

3.4 use the Documentation for the purpose of providing you with assistance on the use of the Software and the Hardware;

3.5 transfer the Products and your Licence on a permanent basis to another person only if that person agrees to accept the terms of this Agreement and you either transfer all copies (including the most recent update and all prior versions) to that person or destroy any copies not transferred. If you transfer possession of any part of the Products to another person, your Licence is automatically terminated.

4. PROHIBITIONS

You may not nor may you permit others to:

4.1 use the software in a corporate environment or in conjunction with any information relating to a business other than personal data unless licenced to do so by DES.

4.2 use, copy, distribute, rent, loan, lease, sub-licence, transfer or otherwise deal in the Products (or any of them) except as permitted by this Agreement;

4.3 alter, adapt, merge, modify or translate the Software or the Documentation in any way for any purpose, including, without limitation, for error correction except with express prior permission of DES (which may be withheld at its absolute discretion);

4.4 reverse engineer, disassemble or decompile the Software, software key-file or USB Hardware;

4.5 remove, change or obscure any identification or notices of proprietary rights (including without limit those relating to the Specific Rights) and restrictions on or in the Products (or any of them).

5. TERMINATION

5.1 You may terminate the Licence at any time by deleting all electronic copies of the Software in your control together with any back-up disks and returning the Products together with all copies in any form to DES or the Distributor from which you purchased the same. Any use of any copies of the Products after termination of the Licence is unlawful.

5.2 Your Licence to use the Products will terminate automatically if you:

5.2.1 fail to comply with any term of this Agreement; or

5.2.2 become bankrupt, go into liquidation, suffer or make any winding up petition, make an arrangement with your creditors, have an administrator. administrative receiver or receiver appointed or suffer or file any similar action.

5.3 Upon termination of the Licence for any reason you will delete all electronic copies of the Software in your control together with any back-up disks and return the Products together with all copies in any form to DES or the Distributor from which you purchased the same. Any use of any copies of the Products after termination of the Licence is unlawful.

6. LIMITED WARRANTY

6.1 Subject to clause 6.2 and clause 8.4 DES warrants only to you as the original licensee that for a period of 12 months from the date upon which you purchased the Products, the Software and the Hardware when used properly will in all material respects provide the functions and facilities as described in the Documentation.

6.2 DES' entire liability and your exclusive remedy under the warranty given in clause 6.1 will be (at DES' absolute option) to either:

6.2.1 repair or replace the Products (if any) which does not conform with the warranty; or

6.2.2 refund the price paid for the Products and terminate the Licence. This remedy is subject to the return of the Products with a copy of your payment receipt to DES not later than 14 days after the end of a period of 12 months from your purchase of the Software.

7. EXCLUSION OF OTHER WARRANTIES

7.1 Subject to the express warranties given pursuant to clause 6, DES make and you receive no other warranties, conditions or representations, express or implied, statutory or otherwise, and without limitation the implied terms of satisfactory quality and fitness for a particular purpose are excluded. DES does not warrant that the operation of the Products will be error free or uninterrupted. It is your responsibility to ensure that the Products are suitable for your needs and the entire risk as to the performance and results of the Products is assumed by you.

7.2 You acknowledge and accept that:

7.2.1 it is your responsibility to protect, maintain and back-up Information;

7.2.2 you should fully back-up all information and data (including without limit any critical information and data) on your computer before installation of the Software and initial use;

7.2.3 you should make back up copies of all encryption keys and key-files and other data generated and stored within a primary USB Hardware key either to other storage media or to a secondary back up USB Hardware key or to a secondary master USB Hardware key held by an administrator;

7.2.4 you are responsible for the use of the Products. DES shall not be liable for any loss, claim or damage suffered as a consequence of any unauthorised or mistaken encryption or decryption of information or data (including without limit, Information) wheresoever and howsoever that information or data is stored;

7.2.5 whilst DES has taken all reasonable steps to ensure the integrity and security of the Hardware and Software, the Products (or any of them) must not be used in any area which is dependent on a fail-safe level of security or is potentially hazardous or dangerous including without limitation nuclear facilities, aircraft navigation, control or communication systems, weapon and defence systems and life support or life monitoring systems;

7.2.6 it is your responsibility to ensure that the level of security and encryption provided by the Products is adequate for your requirements;

7.2.7 you are responsible for your use of the Products (or any of them) including without limit ensuring that such use complies with all applicable laws and regulations of the United Kingdom or such other country, region or State where the Product is used. You must ensure that prior to any use of the Products you have ensured that it is not in contravention of any Government (in the United Kingdom or otherwise) embargo;

7.2.8 it is your responsibility to protect and maintain the USB Hardware. DES shall not be responsible for any loss, damage, expense or claim arising from the loss, theft, misuse, corruption, damage or destruction of the USB Hardware.

8. DISCLAIMER

8.1 Notwithstanding anything to the contrary in this Agreement DES does not exclude or limit liability for death or personal injury resulting from an act or negligence of DES.

8.2 DES will not be liable for any direct, consequential, incidental, or special damage or loss, damage or claim of any kind (including without limitation loss of profits, loss of contracts, business interruptions or loss of, unauthorised or mistaken disclosure or corruption to Information and/or data) however caused and whether arising under contract, tort, including negligence, or otherwise in respect of the Products and your use of them (including without limit any "beta" product provided pursuant to clause 8.4 below).

8.3 If any exclusion, disclaimer or other provision contained in this Agreement is held invalid for any reason and DES becomes liable for loss or damage that could otherwise be limited, such liability, whether in contract, negligence or otherwise, will not exceed the amount actually paid by you for the Products.

8.4 Any Products (including any supporting hardware, software, data or information) supplied by DES or its Distributors as a "beta" product are provided "as is" and are to be used for evaluation purposes only. Under no circumstances should any "beta" product provided pursuant to this clause be used in conjunction with any confidential, critical or important information or data;

8.5 You acknowledge that the allocation of risk in this Agreement is fair and reasonable in all the circumstances and that it is not within DES' control how and for what purposes the Products are used by you.

9. INDEMNITY

You will fully indemnify DES against any loss, damage, expense (including without limit any legal fees) or claim incurred as a consequence of you failing to adhere to any of the terms of this Licence.

10. GENERAL

10.1 This Agreement is the entire agreement between you and DES and supersedes any other oral or written communications, agreements or representations with respect to the Products.

10.2 If any part of this Agreement is held by a court of competent jurisdiction to be unenforceable the validity of the remainder of the Agreement will not be affected.

10.3 This Agreement is governed by the laws of England and Wales and the parties submit to the exclusive jurisdiction of the English Court.

10.4 Except as otherwise expressly stated herein, nothing in this Agreement confers any rights on any person (other than the parties hereto) pursuant to the Contracts (Rights of Third Parties) Act 1999.

10.5 The waiver by DES of any breach or failure to enforce any of the terms and conditions of this Agreement at any time shall not in any way affect, limit or waive DES' rights thereafter to enforce and compel strict compliance with every term and condition of this Agreement.

11. ADDITIONAL RIGHTS FOR CONSUMERS

The following provisions are applicable if you are purchasing the Products as a consumer and by means of a distance contract. For the purpose of this clause "consumer" and "distance contract" shall have the same meaning as set out in the Consumer Protection (Distance Selling) Regulations 2000.

11.1 The price paid for the Products includes the cost of delivering the same to you and all applicable taxes.

11.2 The price must be paid in full before the Products are despatched to you. DES will use its reasonable endeavours to deliver the Products to you within 14 days from the date of payment.

11.3 Notwithstanding anything to the contrary in this Agreement, you have the right to cancel this Agreement at anytime within 7 working days from the date you receive the Products. Should you exercise your right to cancel pursuant to this clause you should immediately return the Products unused, undamaged and fully intact by recorded delivery to DES (at the address set out at in clause 1.1 ("DES") of this Agreement). You are responsible for the cost of returning any Products no longer required pursuant to this clause. DES will refund any monies paid by you to DES within 14 days of receipt of the Products in accordance with this clause (or within 30 days from the date of such cancellation whichever is the earlier).

11.4 If you have any complaints about the Products or DES these should be reported in writing to:

Quality Manager
Data Encryption Systems Limited
Silver Street House
Silver Street
Taunton
Somerset
TA1 3DL
England

11.5 DES gives no guarantees, warranties or after sales service other than as set out in this Agreement.

11.6 Nothing in this Agreement will affect the statutory rights of a consumer in 'consumer transactions' under any applicable statute.

Contents

1. Overview 1
    1.1 Introduction 1
        1.1.1 3DES 2
        1.1.2 Blowfish 2
        1.1.3 AES 2
        1.1.4 RSA 2
    1.2 Encryption Algorithm Types 3
        1.2.1 Symmetric Algorithms 3
        1.2.2 Asymmetric Algorithms 3

2. Installation Guide 5
    2.1 DESlock$^+$ Components............................ 5
    2.2 Minimum System Requirements 6
    2.3 Installation Overview 7
        2.3.1 Install the DESlock+ Software 7
        2.3.2 Install the Backup DESkey 8
        2.3.3 Configure the Backup DESkey 9
        2.3.4 Install the User DESkey 9
        2.3.5 Configure the Key-File 10

3. DESkey Setup Wizard.. 11
    3.1 Typical Single User Setup 13
    3.2 Advanced Single user Setup 17
    3.3 Corporate Setup 22
        3.3.1 Admin Stage............................. 22
        3.3.2 User Stage 26
    3.4 Key-File 29

4. Activating DESlock$^+$.. 33
    4.1 Using DESlock$^+$ 34
    4.2 Menu Options....................................... 35
        4.2.1 About..................................... 35
        4.2.2 Key Management 35
        4.2.3 Key Transfer.............................. 35
        4.2.4 Key Transfer Database................. 35
        4.2.5 Control Panel............................. 35
        4.2.6 Scratch Pad 35
        4.2.7 Mount Manager 35
        4.2.8 Switch DESkey 36
        4.2.9 Deactivate 36
        4.2.10 Exit.. 36

5. Backup Configuration Wizard 37

6. Terminator and Group Codes 41
- 6.1 Description 41
- 6.2 Terminator Code Example 41
- 6.3 Group Code Example 42

7. DESlock$^+$ Control Panel 43
- 7.1 General 44
- 7.2 Timeout 46
- 7.3 Hot Keys 47
- 7.4 Keys 47
- 7.5 Passwords 49
- 7.6 Backup 50
- 7.7 Administration 52
- 7.8 Software Token 53

8. Encryption Key Manager 55
- 8.1 Key Storage 56
  - 8.1.1 Key Slot 56
  - 8.1.2 Name 56
  - 8.1.3 Type 56
  - 8.1.4 Length 56
  - 8.1.5 Terminator Code 57
- 8.2 Options 58
  - 8.2.1 Delete 58
  - 8.2.2 Rename 58
  - 8.2.3 Make Default 58
  - 8.2.4 Send To 59
  - 8.2.5 Backup 60
  - 8.2.6 Generate 62
  - 8.2.7 Restore 62

9. Key Generation Wizard 63
- 9.1 Generating a new encryption key 63

10. Key Transfer Database 67

11. Key Transfer Wizard 69
- 11.1 Transferring Encryption Keys 70
  - 11.1.1 Request 71
  - 11.1.2 Issue 72
  - 11.1.3 Update 75

12. Encrypting with DESlock$^+$ 77
- 12.1 Folder Encryption 77
  - 12.1.1 Network Shares 81
- 12.2 Individual File Processing 82
  - 12.2.1 Encrypt Files 82
  - 12.2.2 Decrypt Files 83
  - 12.2.3 Process Files 83
- 12.3 DESlock$^+$ Tools 84
- 12.4 Offline Encrypted Folders 86

13. Mount Manager 89
13.1 Create Mountable File 89
13.1.1 CD Autorun.............................. 92
13.2 Using Mountable Files 93
13.2.1 Shared Access.......................... 93
13.2.1 File Sharing 93
13.2.1 Dismounting Volumes 93
13.3 Encryption Key Caching 94

14. DESlock+ Archive.. 95

15. Outlook Plug-in 99
11.1 Outlook Integration 99
11.1.1 Email Options 100
11.1.2 Encrypting a message................ 101
11.1.3 Message Properties 104
11.1.4 DESlock+ Message Viewer........... 105
11.1.5 DESlock+ Configuration 106
11.2 Key Transfer....................................... 108

16. Scratch Pad 109

DESlock+ Manual Version 2.20.3

Overview

Introduction

DESlock$^+$ is a data encryption tool designed to provide fast and transparent protection to files and folders on a Windows client or server PC. It can be used to protect any data including personal files, corporate information, confidential records or email.

The ability to use common encryption keys means that DESlock$^+$ users are able to work with shared encrypted data. By using a common key, a workgroup can edit and update shared files within an encrypted folder on a network drive without the need to decrypt and re-encrypt the files whilst working.

Data can be encrypted to and from any storage device on the host PC using one of several proven and trusted encryption algorithms. Up to 64 encryption keys are stored within the hardware of a DK5 DESkey and are only available for use after entering a secure user definable password or phrase. Software based Key-Files provide only a single encryption key.

Encryption keys can be securely transferred between DK5 DESkeys and the entire process is taken care of by a simple user wizard. The powerful RSA public-key algorithm is used within the DESkey itself to encrypt and decrypt encryption key data. By using hardware based public key cryptography, encryption key data is well protected during transmission between users even over insecure channels. Encryption keys cannot be transferred between Key-Files.

Key management and administration when using DESlock$^+$ with a DK5 is controlled using protected settings within the DESkey hardware. Once a DESkey is configured, its permissions are the same from one PC to the next. In addition unique key propagation controls make it possible to control the range and scope of key sharing within workgroups.

Encryption Algorithms

DESlock$^+$ currently supports three algorithms to perform encryption of files and folders. The Key Generation Wizard allows the encryption type to be specified from the list, but a Key-File can only supports Blowfish. These available encryption algorithms are:

3DES

3DES (Triple DES) is a variant form of the DES (Data Encryption Standard) algorithm, originally developed by IBM in 1974. 3DES uses 2 56-bit keys, giving an effective key length of 112 bits, and performs DES encryption on the data three times using these keys.

Blowfish

The Blowfish algorithm was developed in 1993 by Bruce Schneier, President of a consulting firm specialising in computer security, and author of Applied Cryptography. Blowfish is a 64-bit block cipher with a single 128-bit encryption key.

AES

AES (Advanced Encryption Standard) was developed as a new encryption standard to replace DES. Rijndael was accepted as the AES algorithm on October 2, 2000. The Rijndael algorithm was developed by Joan Daemen and Vincent Rijmen, Belgian cryptographers who gained PhDs at the computer security and industrial cryptography labs at Universiteit Leuven. DESlock$^+$ only supports AES with a key length of 128-bits.

Key Exchange Algorithm

DESlock$^+$ also uses the RSA algorithm and Public Key cryptography techniques for all key transfer operations. This allows encryption keys to be securely transferred even via insecure communication channels e.g. the Internet. Encryption keys can only be transferred between DK5 DESkeys, and not Key-Files.

RSA

The RSA asymmetric algorithm was named after Ronald Rivest, Adi Shamir and Leonard Adelman, Computer Science researchers at the Massachusetts Institute of Technology, who developed and patented the algorithm in 1977.

Encryption Algorithm Types

Symmetric algorithms

Symmetric algorithms are those where the same key is used for both encryption and decryption or where one key can be calculated given knowledge of the other. The security of these algorithms rests entirely within the key which means that if encrypted messages are to remain secret then the key must be kept secret. Generally the algorithm used is made available in the public domain so that it can be inspected and judged on its security.

Symmetric algorithms come in two different forms, a stream cipher and a block cipher.

Stream Cipher

Stream ciphers operate on data on a bit by bit (or byte by byte) basis. This means data can be encrypted as it is passed through the algorithm.

Block cipher

Block ciphers operate on data in blocks or a number of bits. These algorithms require a complete block to be available before it can be encrypted. Typically the block size is 64 bits.

Asymmetric algorithms

Asymmetric algorithms, or public key algorithms, are those where two keys are needed: one used for encryption and one used for decryption. Also, the decryption key cannot be calculated given knowledge of the encryption key, at least not in any reasonable length of time.

The security lies in the fact that it is not viable to calculate the decryption key (the private key) from the encryption key (the public key). Therefore the public key can be widely distributed so anyone can encrypt data but only the person with knowledge of the private key can decrypt the data.

This page has been intentionally left blank

Installation Guide

DESlock$^+$ Components

DESlock$^+$ can be used with hardware tokens known as DK5 DESkeys, or with a software based Key-File. DESlock$^+$ may be downloaded freely from our website www.deslock.com, or is included with a DESlock$^+$ sales pack. Key-Files can be downloaded from our website. Please review the licensing information for restrictions on use of Key-Files.

A copy of DESlock$^+$ using a Key file can be used with hardware tokens at any time if they are available. A DESlock$^+$ sales pack and additional DK5s can be purchased online or by calling our sales department.

A DESlock$^+$ sales pack will contain the following items. Please follow the installation instructions carefully before trying to use DESlock$^+$.

- 2 Identical DK5 USB DESkeys
- DESlock$^+$ software and driver CD
- DESlock$^+$ User Manual
- USB extension cable

NOTE: There are two identical DK5 USB DESkeys supplied with the DESlock$^+$ sales pack. One of the DESkeys is intended to be the 'User' DESkey for everyday use. The second is intended to be a 'Backup' DESkey, to be kept as a means to backup important encryption keys. This safeguards access to encrypted data should the User DESkey ever be lost or damaged.

Once installed, the DESlock$^+$ software provides utilities and wizards to allow, amongst other things, encryption keys to be managed (including generating and transferring keys), a scratchpad to access secure memory within the DESkey and an encryption plug-in for the Microsoft® Outlook® email client.

Minimum System Requirements

DESlock$^+$ requires a minimum specification of machine in order to run effectively. The system should comply with or exceed the specifications listed below:

- Microsoft Windows 98, Windows 98 Second Edition, Windows Me, Windows 2000 Professional, Windows XP Home Edition or Windows XP Professional.
- 64MB of hard-disk space
- CD-ROM Drive
- VGA (640 X 480) or higher resolution monitor with 256 colours or more
- Pointing Device and Keyboard
- Type A USB Port which complies with the USB 1.1 or later specification
- Internet Explorer 4 or later

For Windows 98 or Windows 98 Second Edition:

- Pentium 166MHz
- 32MB of RAM

For Windows Me:

- Pentium 166MHz
- 64MB of RAM

For Windows 2000, Windows XP Home Edition or Windows XP Professional:

- Pentium 300MHz
- 128MB of RAM

DESlock$^+$ will not run on Windows 95 or Windows NT4.

Installation Overview

The installation and setup of DESlock$^+$ comprises the following steps:

Step 1: Install the DESlock$^+$ software

1. Close any other software applications that are running.

2. Remove any inserted DESkeys.

3. Insert the CD into your CD-ROM drive.

4. If the CD does not 'autorun', click the *Start* button then choose *Run* and type:

```
x:\dlpsetup.exe
```

where `x:` is the drive letter associated with your CD-ROM drive.

5. Follow the on-screen prompts to install the software

Note: Once installation is complete, the computer will be restarted before DESlock$^+$ can be used.

6. After rebooting, a new icon will be displayed in the system tray as shown in Figure 2 - 1.

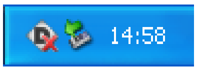


Figure 2 - 1

Step 1b:

If you are only using a Key-File and do not have a DK5 DESkey then skip to Step 5.

Step 2: Install the 'Backup' DESkey

Although it is a fully functional device, the 'Backup' DESkey is intended to be kept safely and only used to store encryption key backups. The process of creating an encryption key backup is covered in detail later in the manual but for now it is sufficient just to setup the key so it is ready to be used.

Insert the 'Backup' DESkey into a free type A USB port. The USB port can be on the PC or on a USB hub connected to the PC.

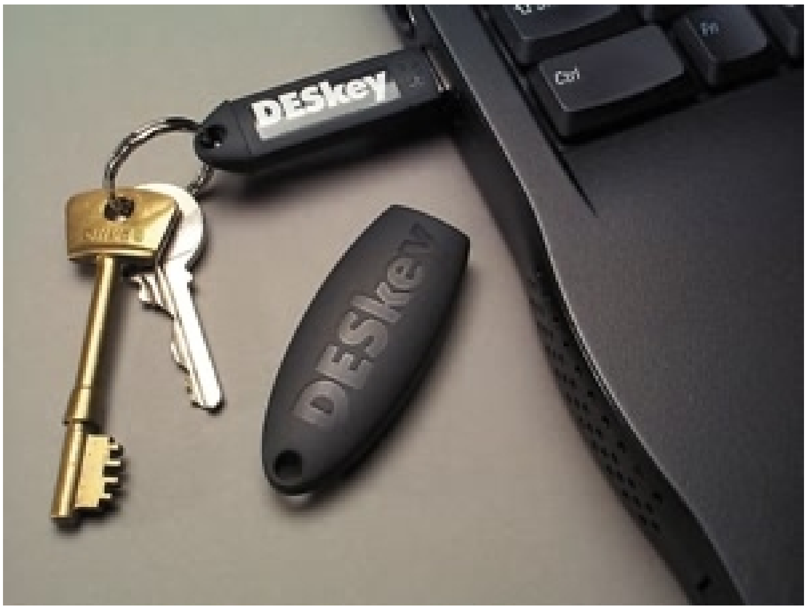
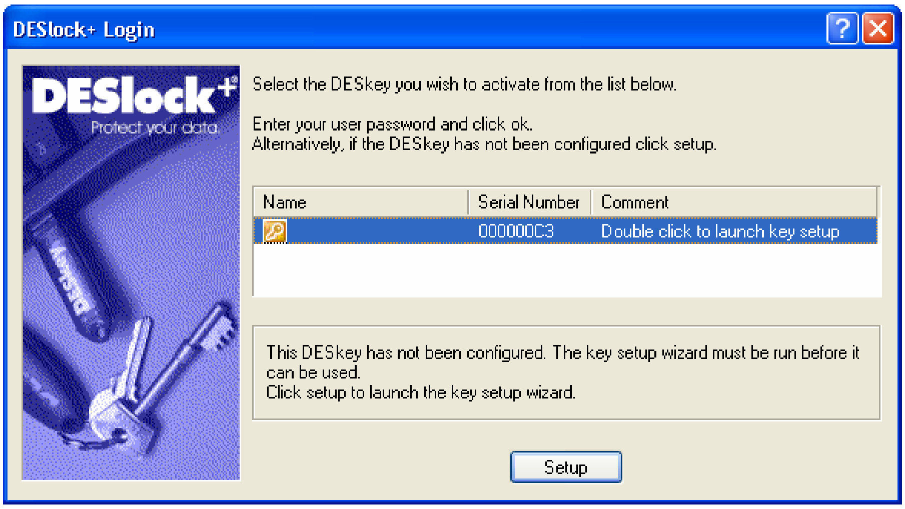


Figure 2 - 2

The hardware should immediately be detected and the DESlock$^+$ login screen will be shown prompting the user to launch the key setup (Figure 2 - 3).



Select the DESkey you wish to activate from the list below.

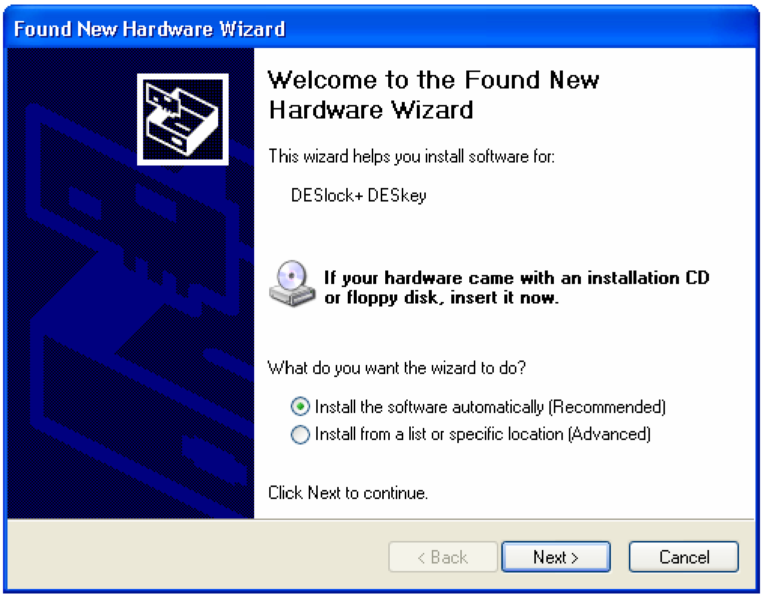
Enter your user password and click ok.
Alternatively, if the DESkey has not been configured click setup.

Name	Serial Number	Comment
	000000C3	Double click to launch key setup

This DESkey has not been configured. The key setup wizard must be run before it can be used.
Click setup to launch the key setup wizard.

Figure 2 - 3

Under Windows XP the new hardware wizard will be displayed the first time the DESkey is inserted into a port and you should click the recommended option for an automatic install.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

DESlock+ DESkey

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

Figure 2 - 4

Step 3: Configure the 'Backup' DESkey

From the login screen, launch the key setup wizard. See the chapter entitled **DESkey Setup Wizard** on page 11 for more information on configuring a DESkey. In most cases the Typical Single User setup would be best for the Backup 'DESkey.' It is not necessary to log into the 'Backup' DESkey after configuring it.

Step 4: Install and Configure the 'User' DESkey

Repeat steps 2 and 3 above using the 'User' DESkey instead of the 'Backup' DESkey.

After the 'User' DESkey has been configured, you may log into it. However, be aware that the **Backup Configuration Wizard** (see page 37) will run each time you activate the DESkey until it has been successfully completed.

Step 5: Configure the Key-File

If you are configuring a DESkey Key-File, the DESkey Setup Wizard may be launched from the DESlock$^+$ Login Box. Refer to the **DESkey Setup Wizard** on page 29 for more information.

DESkey Setup Wizard

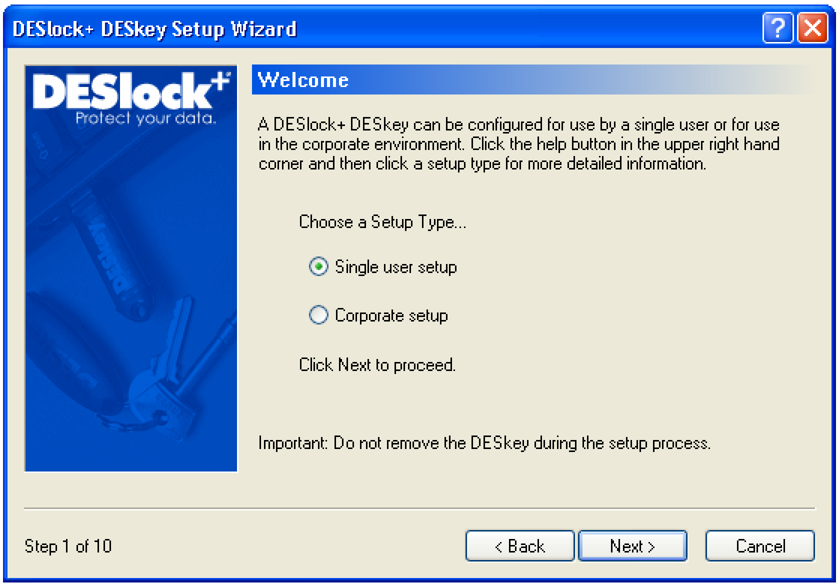
DESlock^{+} can be used with either a hardware DK5 DESkey or a software Key-File. Before either is used however, it must be configured. To configure the DK5 DESkey, see page 11 onwards. To configure a Key-File, see page 29 onwards.

Hardware: DK5 DESkey

Before a DK5 DESkey can be used with DESlock^{+}, it must first be configured. There are two basic configuration methods: a single user setup and a corporate setup.

Once a DESkey has been successfully configured, details of the device will be stored in the local Key Transfer Database (described on page 59). Use of the Key Transfer Database is described in more detail later in the manual.

When the DESkey setup wizard is run, a wizard will be displayed prompting the user to select either the single user or corporate setup type.



A DESlock+ DESkey can be configured for use by a single user or for use in the corporate environment. Click the help button in the upper right hand corner and then click a setup type for more detailed information.

Choose a Setup Type...

● Single user setup

○ Corporate setup

Click Next to proceed.

Important: Do not remove the DESkey during the setup process.

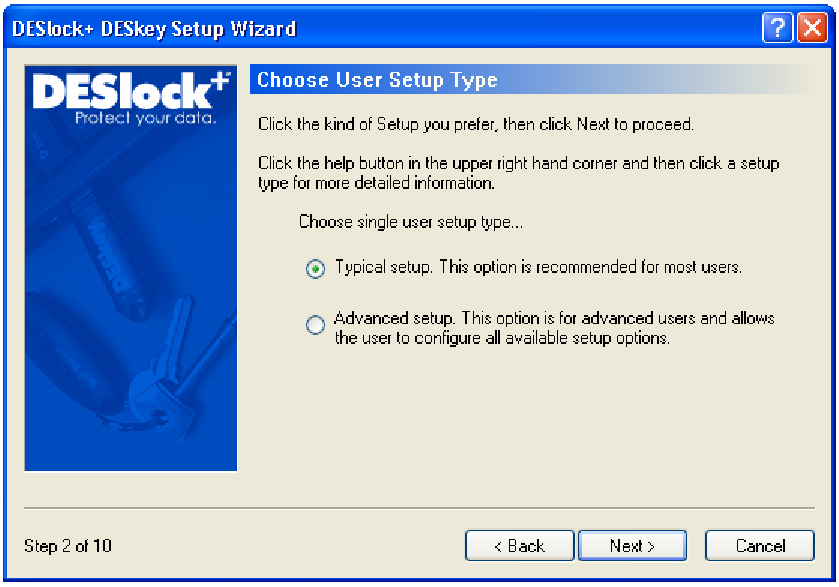
Step 1 of 10

Figure 3 - 1

The single user setup is designed for individuals to easily configure their own DESkey. This is ideally suited for small business and personal use where access to the DESkey does not need to be restricted by an administrator. The DESkey can be setup and used immediately.

Choosing corporate setup will launch the administration stage of the corporate setup. The corporate setup is designed for larger organisations where access to and operation of the DESkey can be restricted. The setup is intended to be run by the administrator who can pre-set various options within the DESkey and can specify the access level of the final user. Before use the DESkey must finally be configured via a final corporate user setup phase.

If the single user setup type is chosen, a further option dialog will be shown. The typical setup is the quickest setup type as default values will be used for certain configuration questions. The advanced setup type will allow the user to configure the DESkey options during the DESkey setup process. These options can be changed after setup is complete using the DESlock$^+$ Control Panel (described in more detail on page 46).



DESlock+ DESkey Setup Wizard

Choose User Setup Type

Click the kind of Setup you prefer, then click Next to proceed.

Click the help button in the upper right hand corner and then click a setup type for more detailed information.

Choose single user setup type...

● Typical setup. This option is recommended for most users.

○ Advanced setup. This option is for advanced users and allows the user to configure all available setup options.

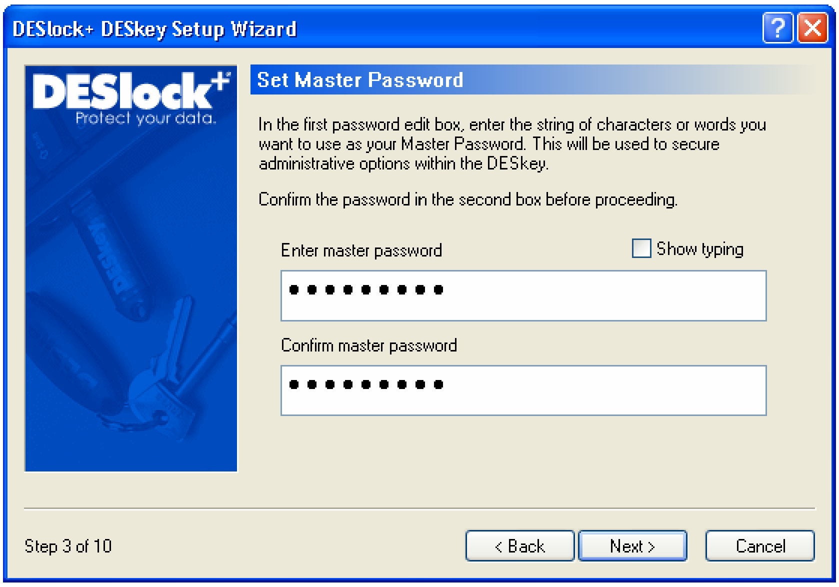
Step 2 of 10

Figure 3 - 2

Both setups are the same. The corporate simply allows the key to be partially setup and finalised by the end user. An alternative would be to do a single user setup and give the DESkey a dummy password the user could change. At the end of the day, there would be no difference.

Typical Single User Setup

Enter an Administrative Master password in the first box and re-enter it in the second box to confirm. The Next button will be disabled until the password has been confirmed. When this has been done, click **Next** to continue.



DESlock+ DESkey Setup Wizard

Set Master Password

In the first password edit box, enter the string of characters or words you want to use as your Master Password. This will be used to secure administrative options within the DESkey.

Confirm the password in the second box before proceeding.

Enter master password ☐ Show typing

●●●●●●●●●●

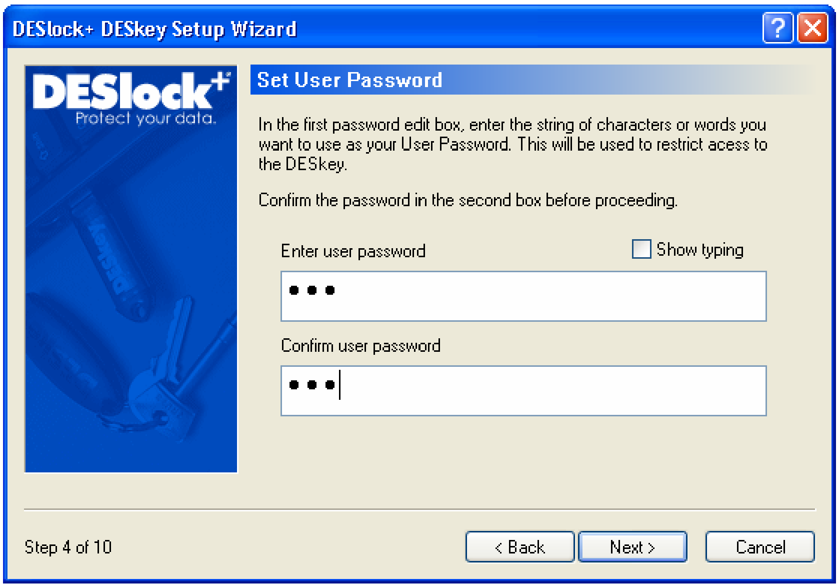
Confirm master password

●●●●●●●●●●

Step 3 of 10

Figure 3 - 3

Enter a User password in the first box and re-enter it in the second box to confirm. The user password will be used to activate the DESkey. When ready, click **Next** to continue.



DESlock+ DESkey Setup Wizard

Set User Password

In the first password edit box, enter the string of characters or words you want to use as your User Password. This will be used to restrict acess to the DESkey.

Confirm the password in the second box before proceeding.

Enter user password ☐ Show typing

●●●

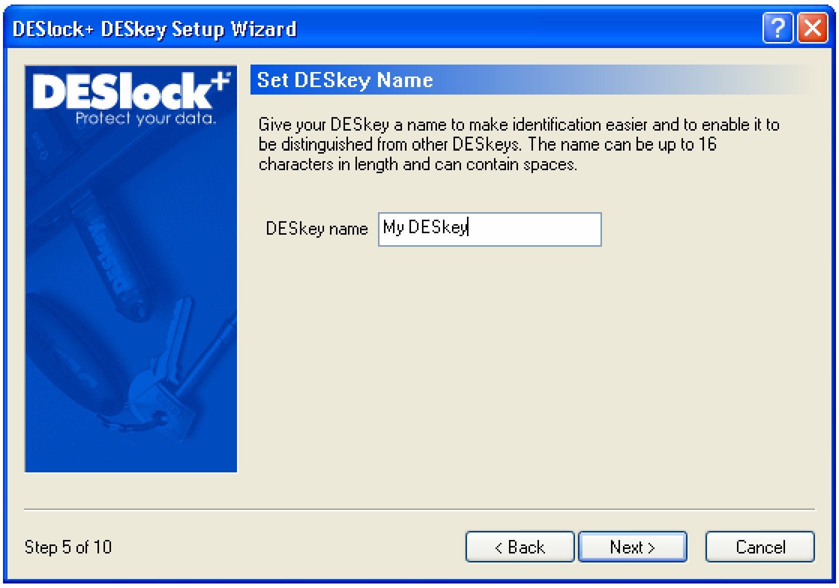
Confirm user password

●●●

Step 4 of 10

Figure 3 - 4

Enter a name to identify the DESkey. This name can be between 1 and 16 characters long and can contain spaces. When a suitable name has been entered click **Next**. The default name is "My DESkey."



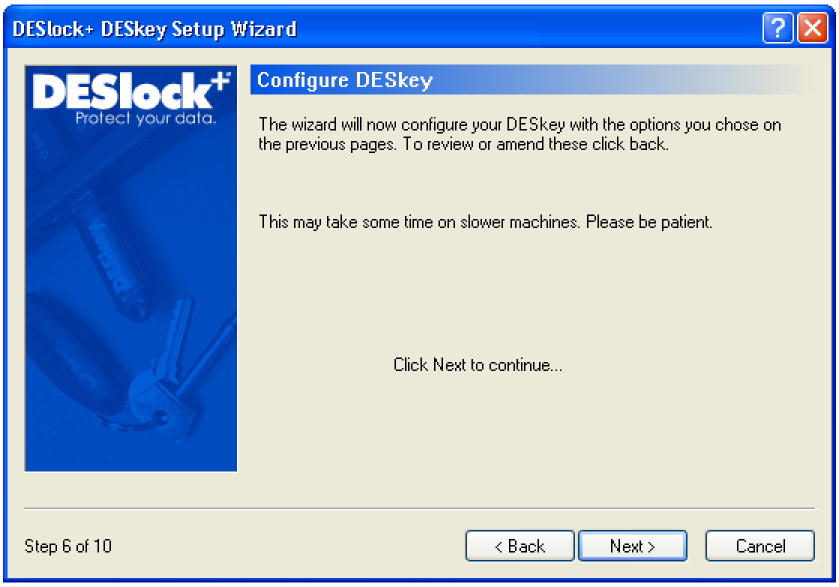
Give your DESkey a name to make identification easier and to enable it to be distinguished from other DESkeys. The name can be up to 16 characters in length and can contain spaces.

DESkey name: My DESkey

Step 5 of 10

Figure 3 - 5

The options you have chosen will now be saved to the DESkey, along with generation of an RSA private and public key pair. Click **Next** to begin this process. The exact length of time required to generate both cannot be predetermined. It is related to the speed of the machine so if running on a slow machine this process could take some time. When complete, click **Next** to proceed.



The wizard will now configure your DESkey with the options you chose on the previous pages. To review or amend these click back.

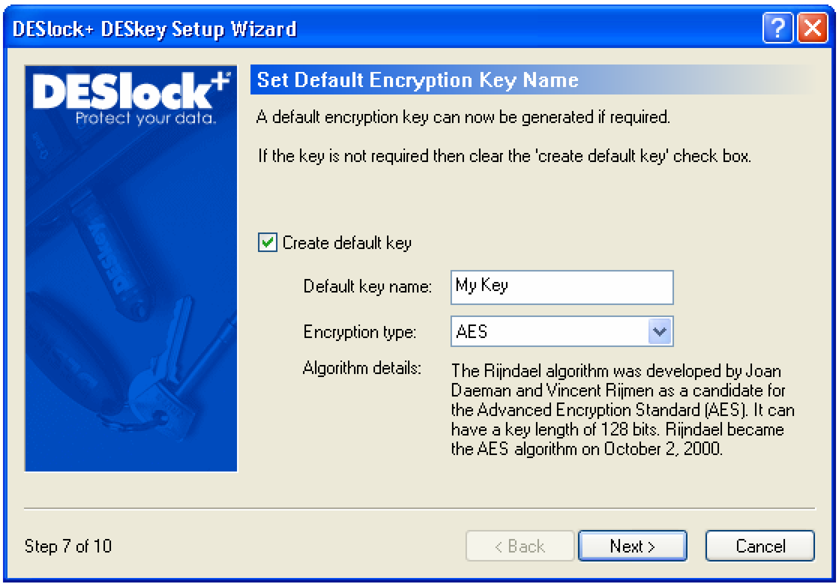
This may take some time on slower machines. Please be patient.

Click Next to continue...

Step 6 of 10

Figure 3 - 6

A default encryption key can now be generated if required. If a key is required at this stage then select the option and enter the desired name and algorithm type. The key will be added to the first slot within the DESkey key space. Click **Next** to continue.



DESlock+ DESkey Setup Wizard

Set Default Encryption Key Name

A default encryption key can now be generated if required.

If the key is not required then clear the 'create default key' check box.

☑ Create default key

Default key name: My Key

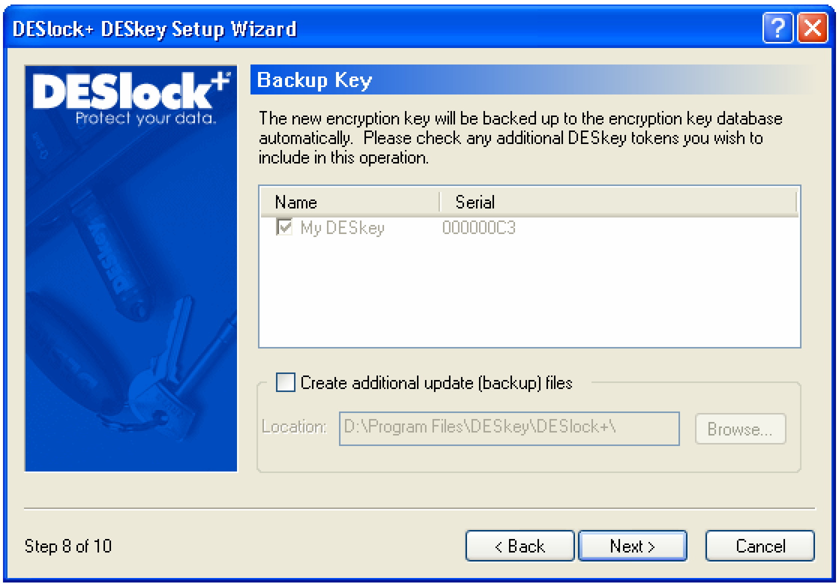
Encryption type: AES

Algorithm details: The Rijndael algorithm was developed by Joan Daeman and Vincent Rijmen as a candidate for the Advanced Encryption Standard (AES). It can have a key length of 128 bits. Rijndael became the AES algorithm on October 2, 2000.

Step 7 of 10

Figure 3 - 7

The newly created encryption key can be backed up at this point if desired. The target DESkey list will contain a list of all connected DESkeys and all DESkeys listed in the Key Transfer Database. The backup process is described in more detail later in the manual on page 52.



DESlock+ DESkey Setup Wizard

Backup Key

The new encryption key will be backed up to the encryption key database automatically. Please check any additional DESkey tokens you wish to include in this operation.

Name	Serial
☑ My DESkey	000000C3

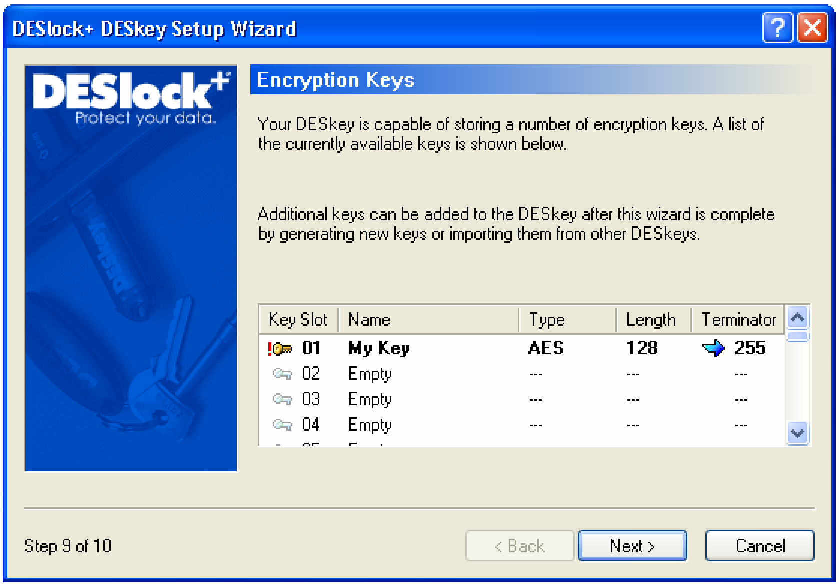
☐ Create additional update (backup) files

Location: D:\Program Files\DESkey\DESlock+\

Step 8 of 10

Figure 3 - 8

If a key was created, it will be displayed below. Click **Next** to continue.



Encryption Keys

Your DESkey is capable of storing a number of encryption keys. A list of the currently available keys is shown below.

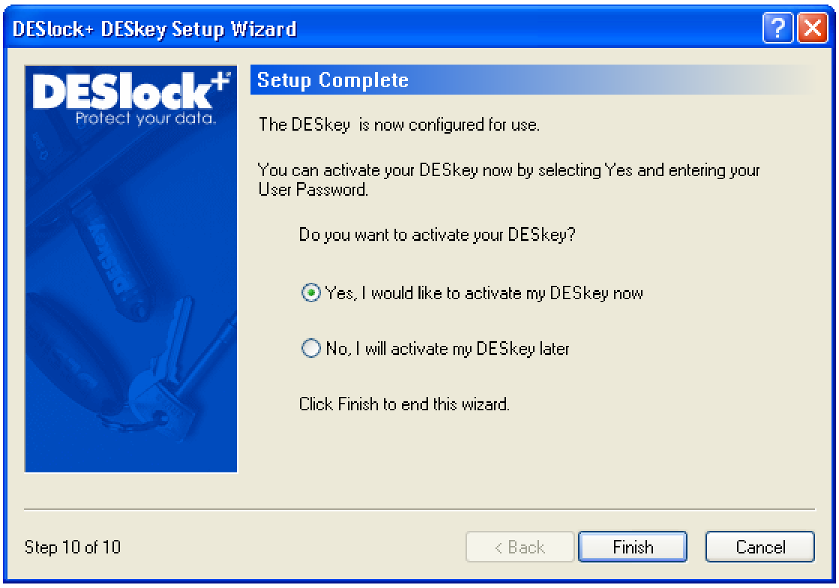
Additional keys can be added to the DESkey after this wizard is complete by generating new keys or importing them from other DESkeys.

Key Slot	Name	Type	Length	Terminator
01	**My Key**	**AES**	**128**	**255**
02	Empty	---	---	---
03	Empty	---	---	---
04	Empty	---	---	---

Step 9 of 10

Figure 3 - 9

The DESkey has now been fully configured for single user use. It can now be activated and used with DESlock$^+$ if desired. Click **Finish** to close the wizard.



Setup Complete

The DESkey is now configured for use.

You can activate your DESkey now by selecting Yes and entering your User Password.

Do you want to activate your DESkey?

● Yes, I would like to activate my DESkey now

○ No, I will activate my DESkey later

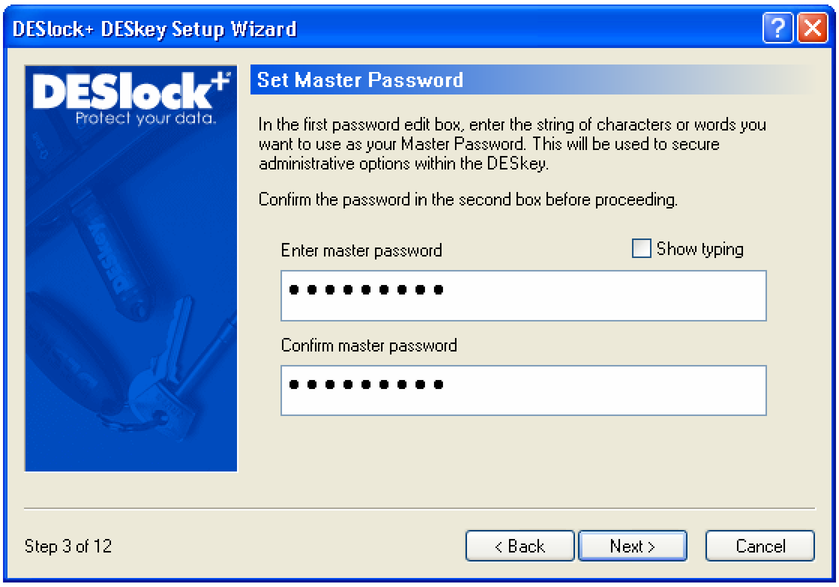
Click Finish to end this wizard.

Step 10 of 10

Figure 3 - 10

Advanced Single User Setup

Enter an Administrative Master password in the first box and re-enter it in the second box to confirm. The next button will be disabled until the password has been confirmed. When this has been done, click **Next** to continue.



DESlock+ DESkey Setup Wizard

Set Master Password

In the first password edit box, enter the string of characters or words you want to use as your Master Password. This will be used to secure administrative options within the DESkey.

Confirm the password in the second box before proceeding.

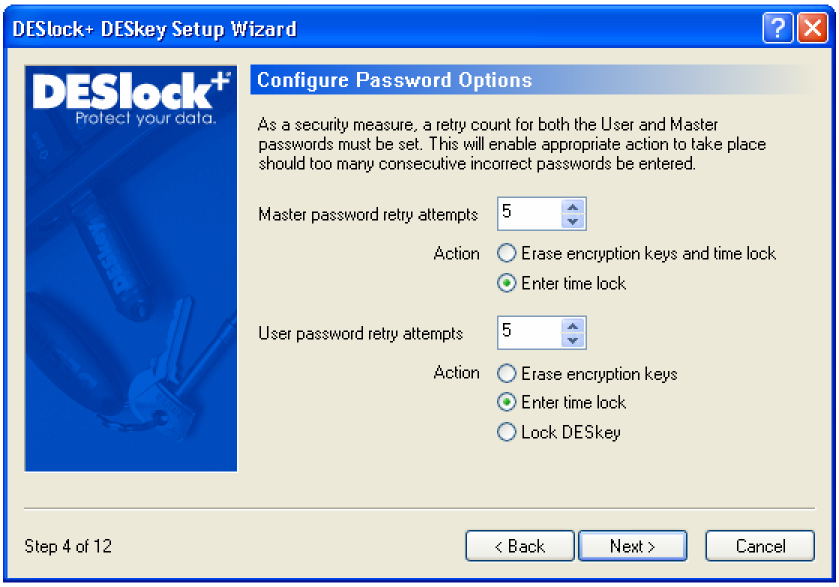
Enter master password: •••••••••• □ Show typing

Confirm master password: ••••••••••

Step 3 of 12

Figure 3 - 11

Enter the allowed number of user and master password retries and resulting action. If the password is entered incorrectly more than the allowed value the DESkey can either erase the DESkey key space, enter a time loop algorithm or lock out the user account. A locked DESkey can only be unlocked using the correct Master password. These settings can be changed at a later date using the DESlock+ Control Panel, as described later on pages 43 and 46.



DESlock+ DESkey Setup Wizard

Configure Password Options

As a security measure, a retry count for both the User and Master passwords must be set. This will enable appropriate action to take place should too many consecutive incorrect passwords be entered.

Master password retry attempts: 5

Action: ○ Erase encryption keys and time lock
● Enter time lock

User password retry attempts: 5

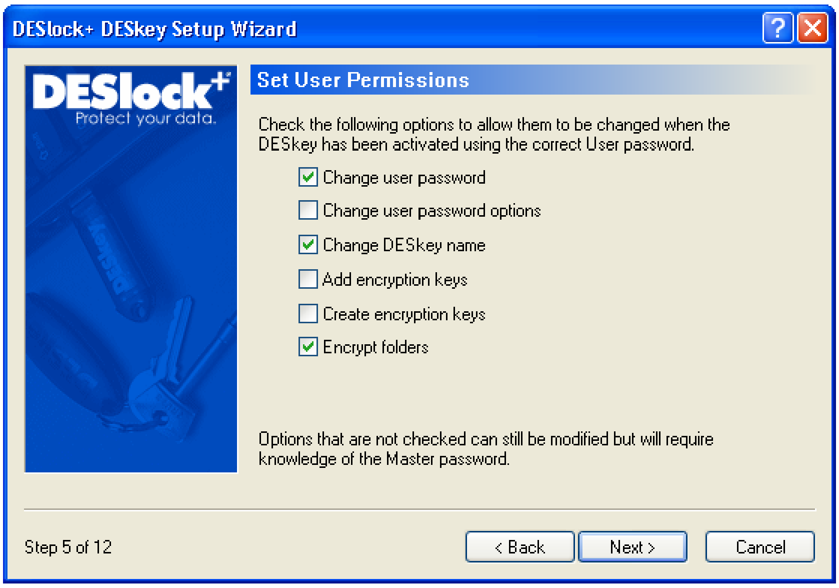
Action: ○ Erase encryption keys
● Enter time lock
○ Lock DESkey

Step 4 of 12

Figure 3 - 12

DESkey functionality can be limited based upon the password entered. Entering the master password will allow all DESkey settings in the list to be modified. Any options that are not checked cannot be changed if logged in as a user. These are:

- Change User Password
- Change User Password Options
- Change DESkey Name
- Add Encryption Keys
- Create Encryption Keys



Set User Permissions

Check the following options to allow them to be changed when the DESkey has been activated using the correct User password.

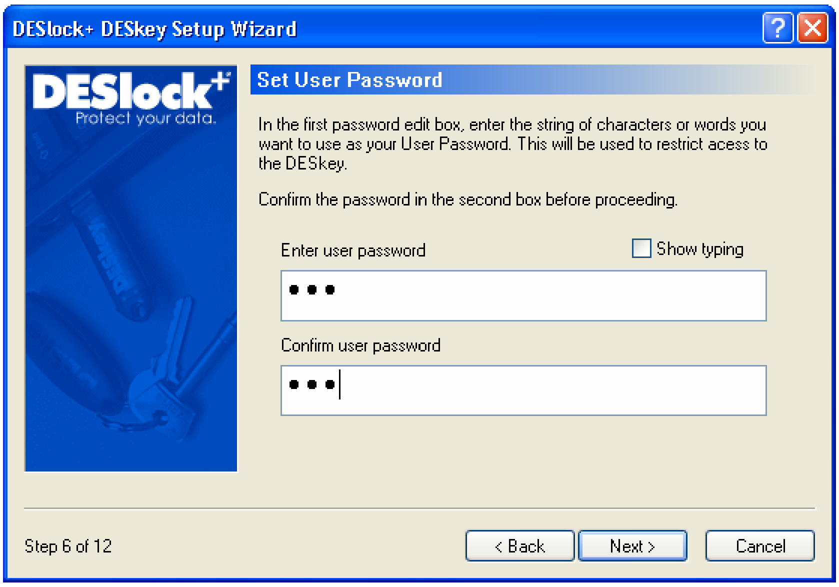
☑ Change user password
☐ Change user password options
☑ Change DESkey name
☐ Add encryption keys
☐ Create encryption keys
☑ Encrypt folders

Options that are not checked can still be modified but will require knowledge of the Master password.

Step 5 of 12

Figure 3 - 13

Enter a User password in the first box and re-enter it in the second box to confirm. The user password will be used to activate the DESkey. When ready, click **Next** to continue.



Set User Password

In the first password edit box, enter the string of characters or words you want to use as your User Password. This will be used to restrict acess to the DESkey.

Confirm the password in the second box before proceeding.

Enter user password ☐ Show typing

●●●

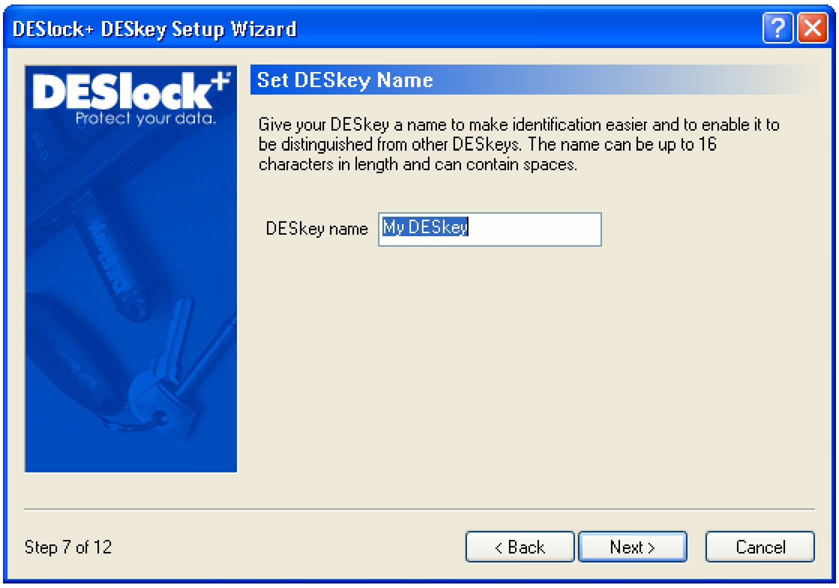
Confirm user password

●●●

Step 6 of 12

Figure 3 - 14

Enter a name to identify the DESkey. This name can be between 1 and 16 characters long and can contain spaces. When a suitable name has been entered click **Next**. The default is "My DESkey".



Set DESkey Name

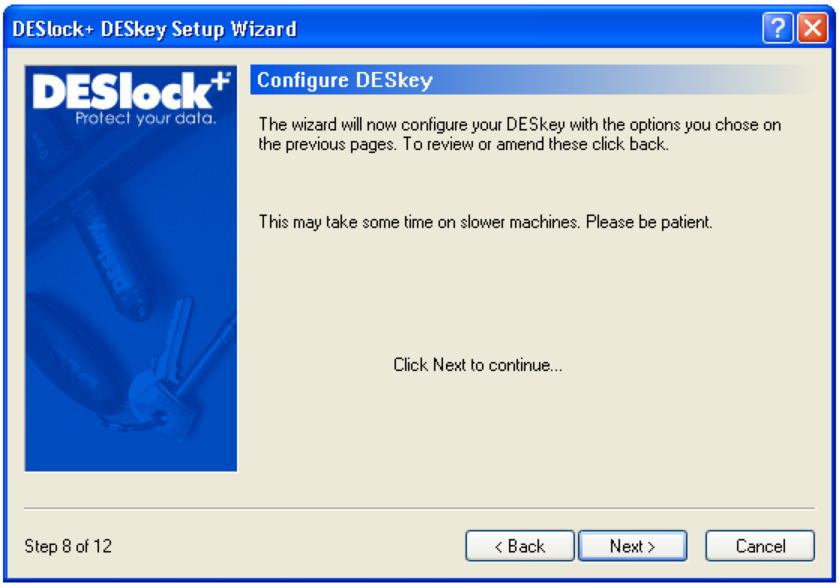
Give your DESkey a name to make identification easier and to enable it to be distinguished from other DESkeys. The name can be up to 16 characters in length and can contain spaces.

DESkey name: My DESkey

Step 7 of 12

Figure 3 - 15

The options you have chosen will now be saved to the DESkey, along with generation of an RSA private and public key pair. Click **Next** to begin this process. The exact length of time required to generate both cannot be predetermined. It is related to the speed of the machine so if running on a slow machine this process could take some time. When complete, click **Next** to proceed.



Configure DESkey

The wizard will now configure your DESkey with the options you chose on the previous pages. To review or amend these click back.

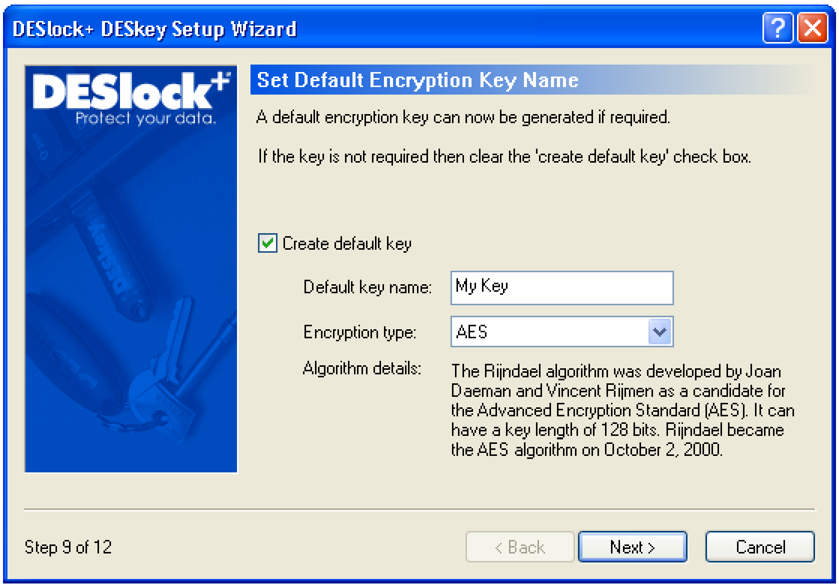
This may take some time on slower machines. Please be patient.

Click Next to continue...

Step 8 of 12

Figure 3 - 16

A default encryption key can now be generated if required. If a key is required at this stage then select the option and enter the desired algorithm type and name. Click **Next** to continue.



Set Default Encryption Key Name

A default encryption key can now be generated if required.

If the key is not required then clear the 'create default key' check box.

☑ Create default key

Default key name: My Key

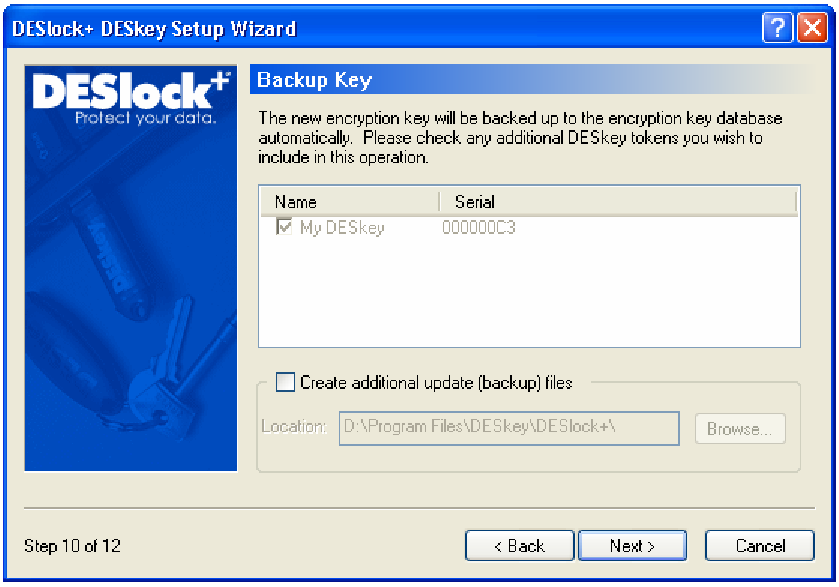
Encryption type: AES

Algorithm details: The Rijndael algorithm was developed by Joan Daeman and Vincent Rijmen as a candidate for the Advanced Encryption Standard (AES). It can have a key length of 128 bits. Rijndael became the AES algorithm on October 2, 2000.

Step 9 of 12

Figure 3 - 17

The newly created encryption key can be backed up at this point if desired. The target DESkey list will contain a list of all connected DESkeys and all DESkeys listed in the Key Transfer Database. The backup process is described in more detail later in the manual on page 52.



Backup Key

The new encryption key will be backed up to the encryption key database automatically. Please check any additional DESkey tokens you wish to include in this operation.

Name	Serial
☑ My DESkey	000000C3

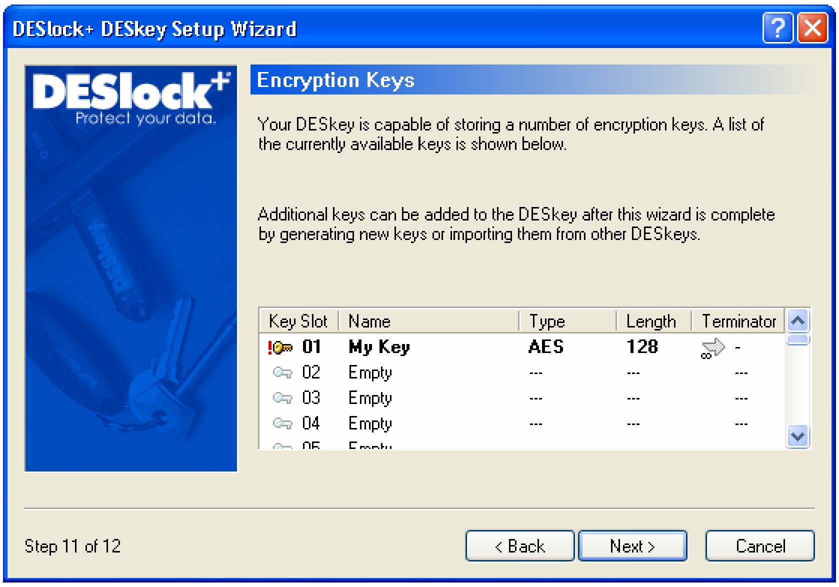
□ Create additional update (backup) files

Location: D:\Program Files\DESkey\DESlock+\

Step 10 of 12

Figure 3 - 18

If a key was created, it will be displayed below. Click **Next** to continue.



DESlock+ DESkey Setup Wizard

Encryption Keys

Your DESkey is capable of storing a number of encryption keys. A list of the currently available keys is shown below.

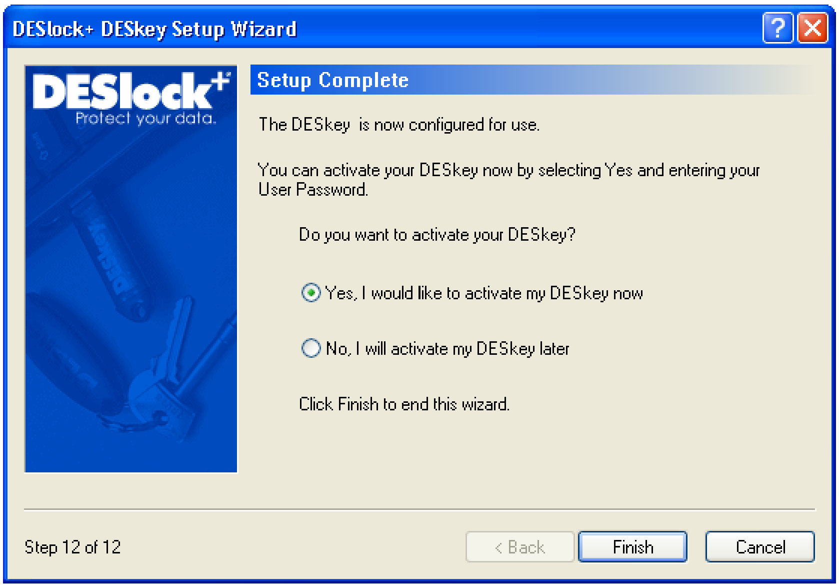
Additional keys can be added to the DESkey after this wizard is complete by generating new keys or importing them from other DESkeys.

Key Slot	Name	Type	Length	Terminator
01	**My Key**	**AES**	**128**	-
02	Empty	---	---	---
03	Empty	---	---	---
04	Empty	---	---	---
05	Empty			

Step 11 of 12

Figure 3 - 19

The DESkey has now been fully configured for single user use. It can now be activated and used with DESlock$^+$ if desired. Click **Finish** to close the wizard.



DESlock+ DESkey Setup Wizard

Setup Complete

The DESkey is now configured for use.

You can activate your DESkey now by selecting Yes and entering your User Password.

Do you want to activate your DESkey?

● Yes, I would like to activate my DESkey now

○ No, I will activate my DESkey later

Click Finish to end this wizard.

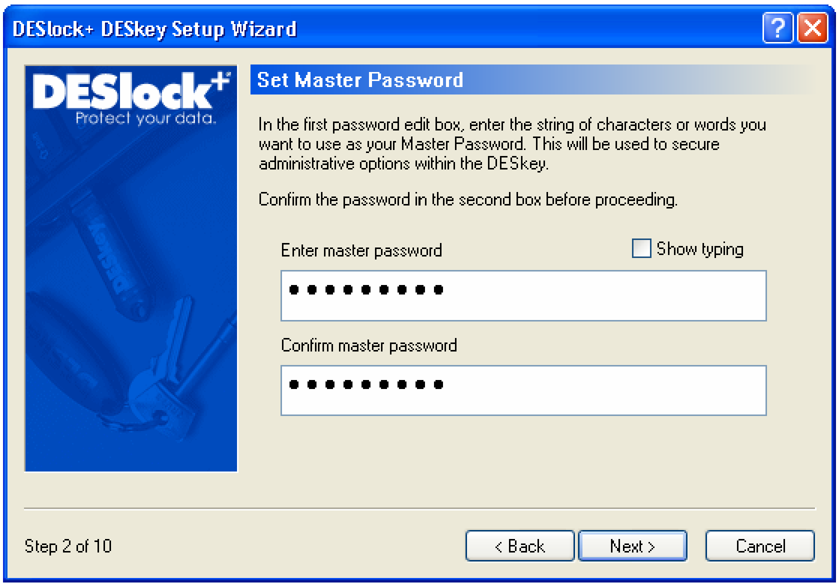
Step 12 of 12

Figure 3 - 20

Corporate Setup

Admin Stage

Enter an Administrative Master password in the first box and re-enter it in the second box to confirm.



Set Master Password

In the first password edit box, enter the string of characters or words you want to use as your Master Password. This will be used to secure administrative options within the DESkey.

Confirm the password in the second box before proceeding.

Enter master password □ Show typing

●●●●●●●●●●

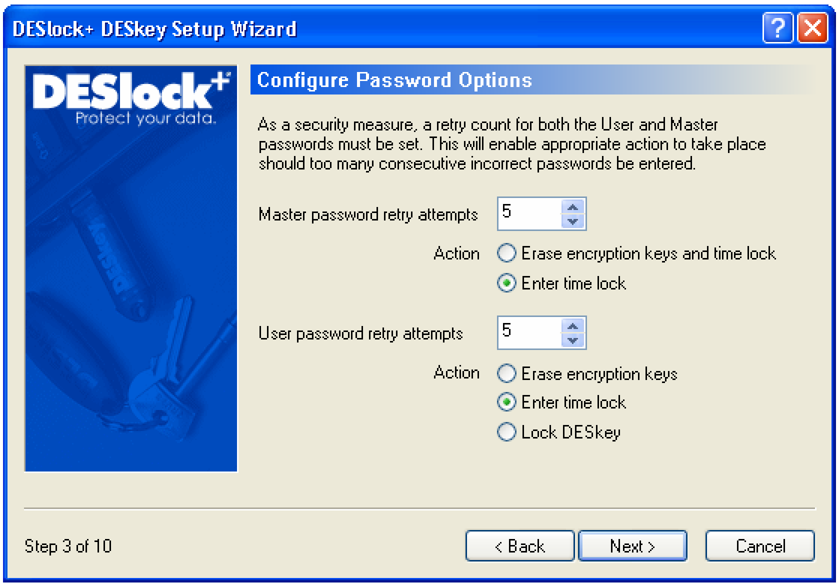
Confirm master password

●●●●●●●●●●

Step 2 of 10

Figure 3 - 21

Enter the allowed number of user and master password retries and resulting action. If the password is entered incorrectly more than the allowed value the DESkey can either erase the DESkey key space, enter a time loop algorithm or lock out the user account. A locked DESkey can only be unlocked using the correct Master password. These settings can be changed at a later date using the DESlock+ Control Panel, as described later on pages 43 and 46.



Configure Password Options

As a security measure, a retry count for both the User and Master passwords must be set. This will enable appropriate action to take place should too many consecutive incorrect passwords be entered.

Master password retry attempts 5

Action ○ Erase encryption keys and time lock
● Enter time lock

User password retry attempts 5

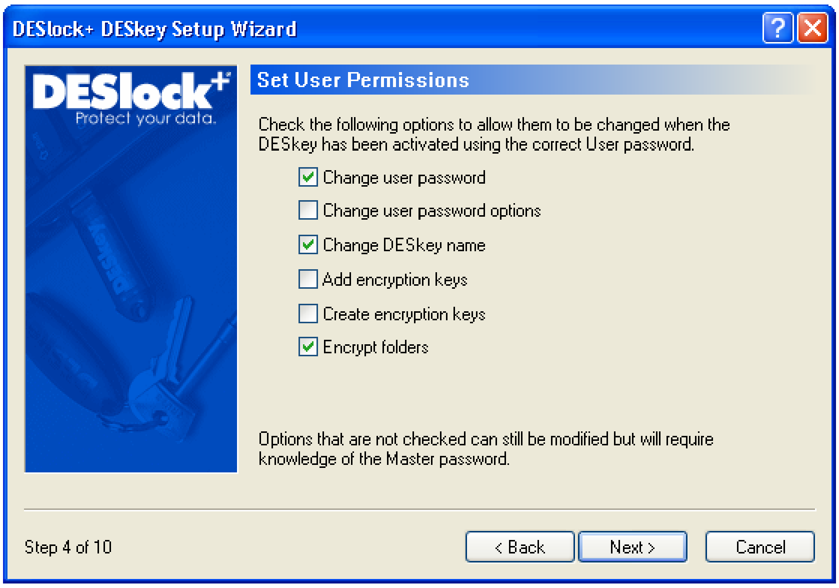
Action ○ Erase encryption keys
● Enter time lock
○ Lock DESkey

Step 3 of 10

Figure 3 - 22

DESkey functionality can be limited based upon the password entered. Entering the master password will allow all DESkey settings in the list to be modified. Any options that are not checked cannot be changed if logged in as a user. These are:

- Change User Password
- Change User Password Options
- Change DESkey Name
- Add Encryption Keys
- Create Encryption Keys



Set User Permissions

Check the following options to allow them to be changed when the DESkey has been activated using the correct User password.

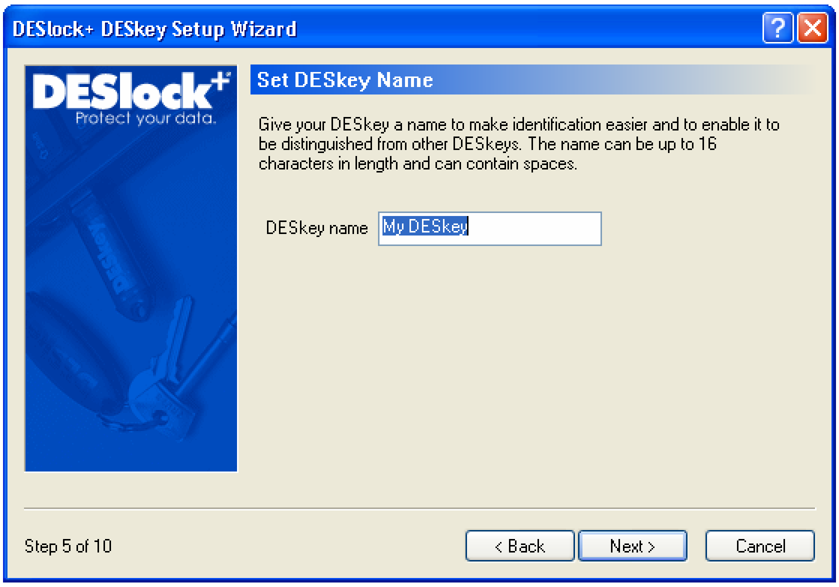
☑ Change user password
☐ Change user password options
☑ Change DESkey name
☐ Add encryption keys
☐ Create encryption keys
☑ Encrypt folders

Options that are not checked can still be modified but will require knowledge of the Master password.

Step 4 of 10

Figure 3 - 23

Enter a name to identify the DESkey. This name can be between 1 and 16 characters long and can contain spaces. When a suitable name has been entered click **Next**. The default is "My DESkey".



Set DESkey Name

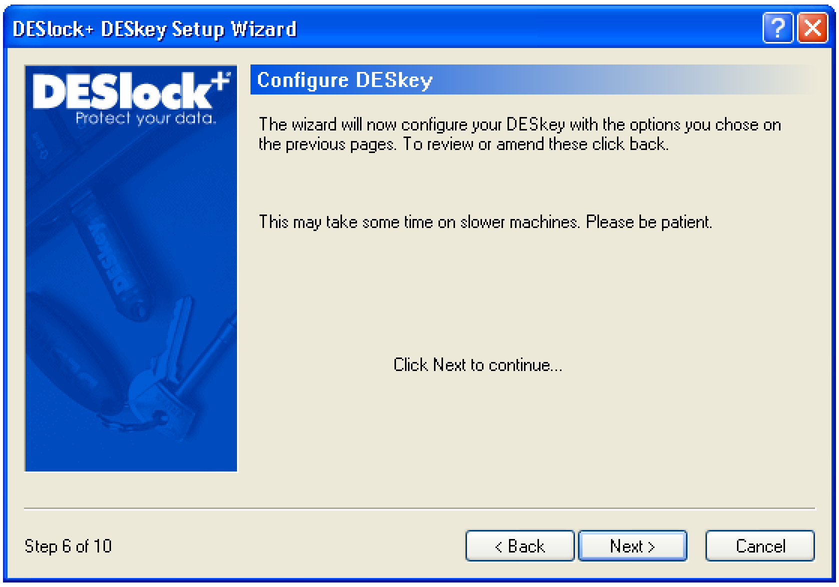
Give your DESkey a name to make identification easier and to enable it to be distinguished from other DESkeys. The name can be up to 16 characters in length and can contain spaces.

DESkey name: My DESkey

Step 5 of 10

Figure 3 - 24

The options you have chosen will now be saved to the DESkey, along with generation of an RSA private and public key pair. Click **Next** to begin this process. The exact length of time required to generate both cannot be predetermined. It is related to the speed of the machine so if running on a slow machine this process could take some time. When complete, click **Next** to proceed.



Configure DESkey

The wizard will now configure your DESkey with the options you chose on the previous pages. To review or amend these click back.

This may take some time on slower machines. Please be patient.

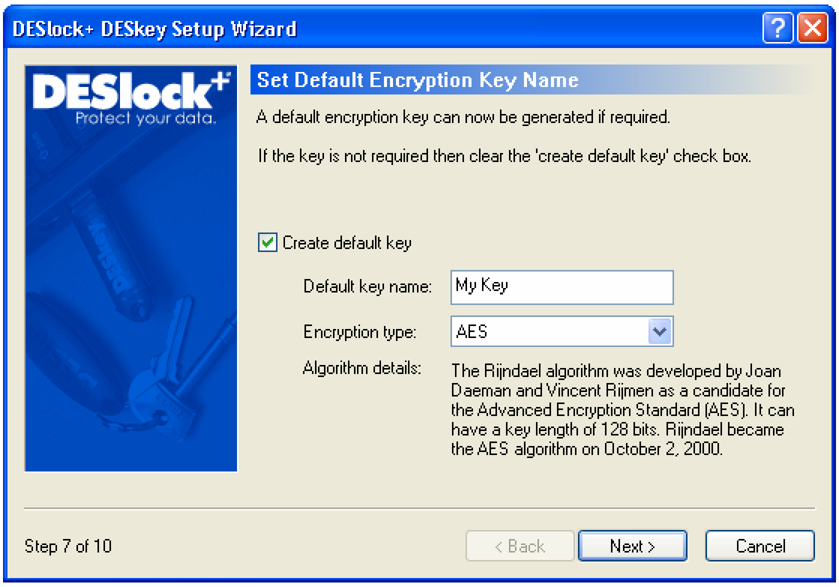
Click Next to continue...

Step 6 of 10

Figure 3 - 25

When the key pair has been generated, click **Next** to proceed.

A default encryption key can now be generated if required. If a key is required at this stage then select the option and enter the desired algorithm type and name. Click **Next** to continue.



Set Default Encryption Key Name

A default encryption key can now be generated if required.

If the key is not required then clear the 'create default key' check box.

☑ Create default key

Default key name: My Key

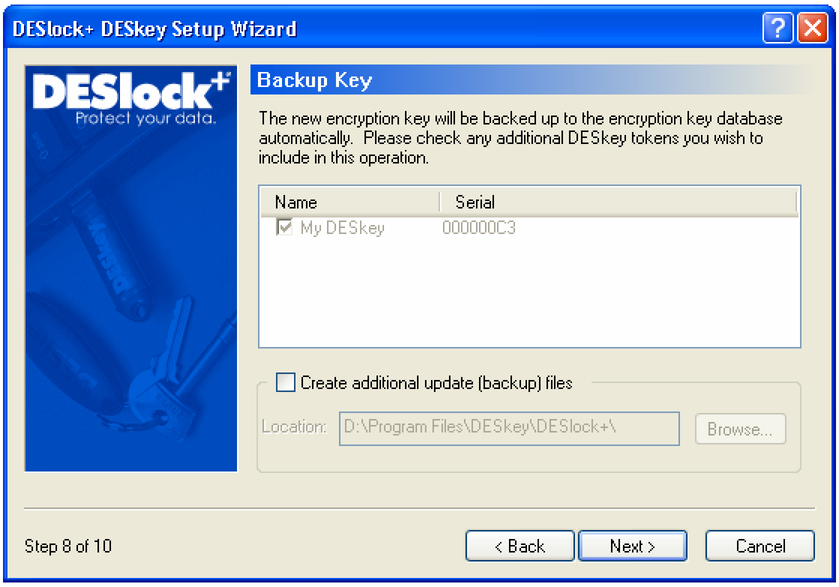
Encryption type: AES

Algorithm details: The Rijndael algorithm was developed by Joan Daeman and Vincent Rijmen as a candidate for the Advanced Encryption Standard (AES). It can have a key length of 128 bits. Rijndael became the AES algorithm on October 2, 2000.

Step 7 of 10

Figure 3 - 26

The newly created encryption key can be backed up at this point if desired. The target DESkey list will contain a list of all connected DESkeys and all DESkeys listed in the Key Transfer Database. The backup process is described in more detail later in the manual on page 52.



The new encryption key will be backed up to the encryption key database automatically. Please check any additional DESkey tokens you wish to include in this operation.

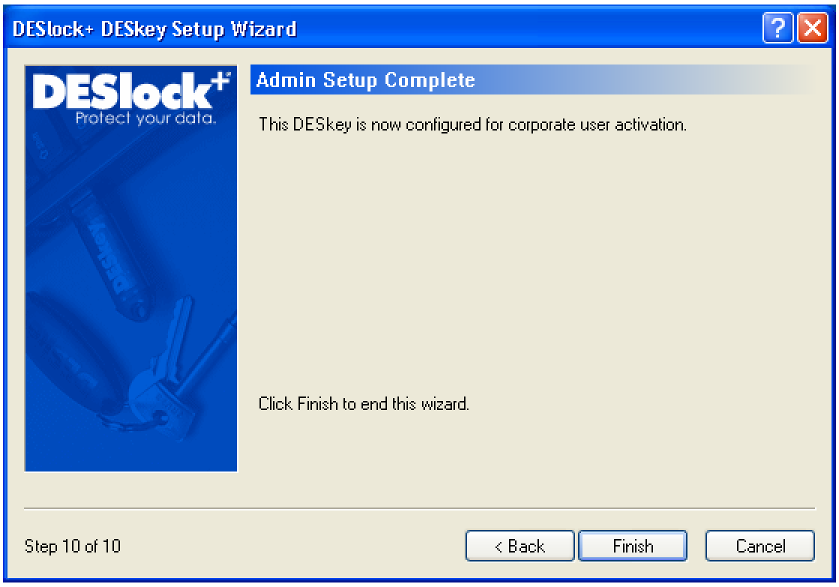
Name	Serial
☑ My DESkey	000000C3

☐ Create additional update (backup) files

Location: D:\Program Files\DESkey\DESlock+\

Figure 3 - 27

The DESkey has now been configured for administration. Before it can be used with DESlock$^+$ it must be finally configured by the end user. Click **Exit** to close the DESkey Setup Wizard.



This DESkey is now configured for corporate user activation.

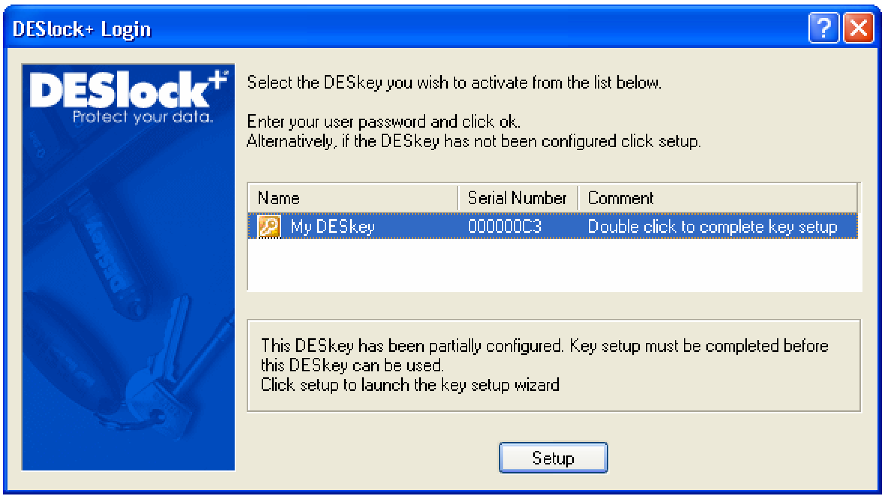
Click Finish to end this wizard.

Figure 3 - 28

User Stage

After the admin stage of the corporate setup, before the DESkey can be used with DESlock$^+$ the user stage setup must also be completed.

When the key is inserted prior to this final stage activation the user will be prompted to complete the DESkey setup process.


DESlock+ Login

Select the DESkey you wish to activate from the list below.

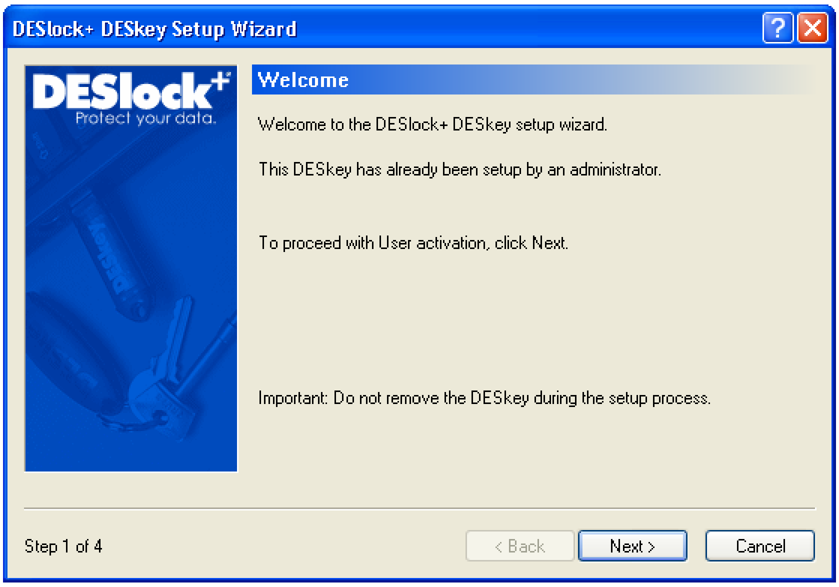
Enter your user password and click ok.
Alternatively, if the DESkey has not been configured click setup.

Name	Serial Number	Comment
My DESkey	000000C3	Double click to complete key setup

This DESkey has been partially configured. Key setup must be completed before this DESkey can be used.
Click setup to launch the key setup wizard

Figure 3 - 29

If selected the final stage setup wizard will run.


DESlock+ DESkey Setup Wizard

Welcome

Welcome to the DESlock+ DESkey setup wizard.

This DESkey has already been setup by an administrator.

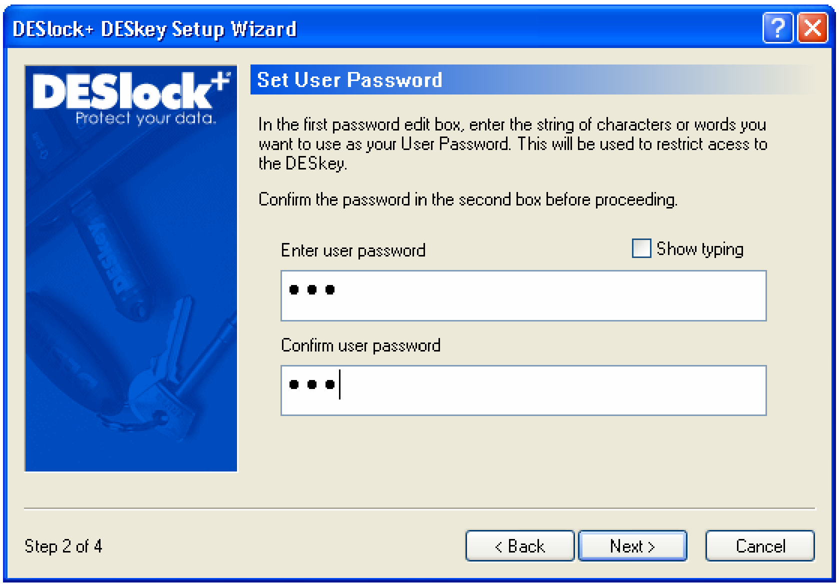
To proceed with User activation, click Next.

Important: Do not remove the DESkey during the setup process.

Step 1 of 4

Figure 3 - 30

Enter a User password in the first box and re-enter it in the second box to confirm. The user password will be used to activate the DESkey. When ready, click **Next** to continue.



Set User Password

In the first password edit box, enter the string of characters or words you want to use as your User Password. This will be used to restrict acess to the DESkey.

Confirm the password in the second box before proceeding.

Enter user password ●●●

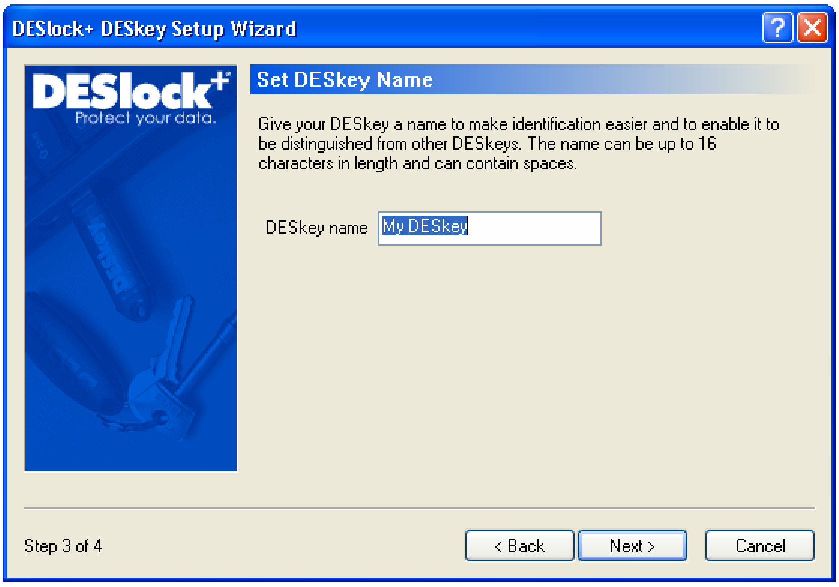
□ Show typing

Confirm user password ●●●

Step 2 of 4

Figure 3 - 31

If the Administrator has allowed the DESkey to be renamed, enter or confirm a name to identify the DESkey. This name can be between 1 and 16 characters long and can contain spaces. The default name was set by the administrator and can be left if desired. When a suitable name has been entered click **Next** to continue.



Set DESkey Name

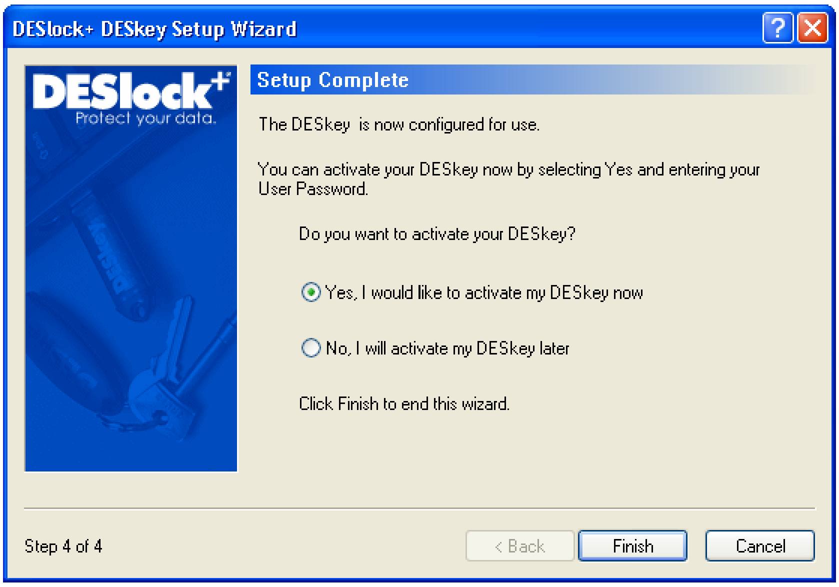
Give your DESkey a name to make identification easier and to enable it to be distinguished from other DESkeys. The name can be up to 16 characters in length and can contain spaces.

DESkey name: My DESkey

Step 3 of 4

Figure 3 - 32

The DESkey has now been fully configured for use. It can now be activated and used with DESlock^{+} if desired. Click **Finish** to close the wizard.



Setup Complete

The DESkey is now configured for use.

You can activate your DESkey now by selecting Yes and entering your User Password.

Do you want to activate your DESkey?

● Yes, I would like to activate my DESkey now

○ No, I will activate my DESkey later

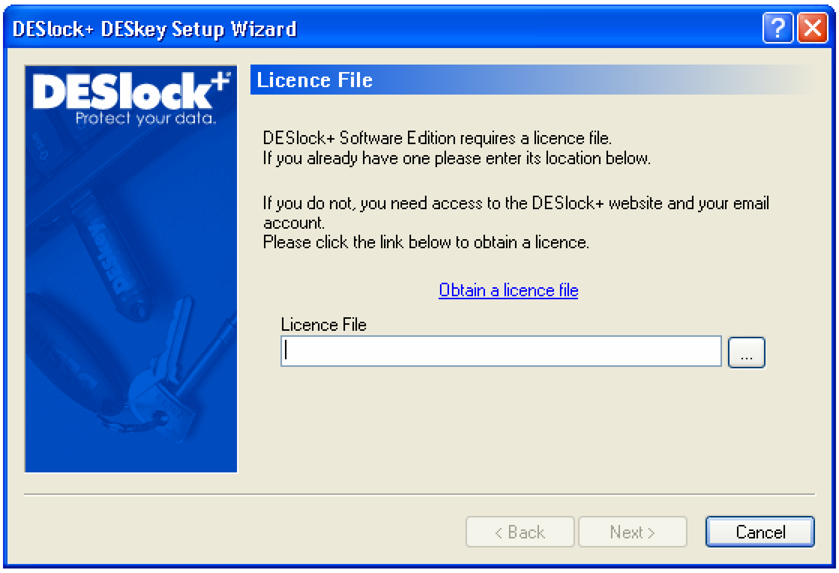
Click Finish to end this wizard.

Figure 3 - 33

Software: Key-File

DESlock$^+$ can be used with an encryption key based upon a Key-File. A Key-File itself is based on two parts of information, namely a licence file and a PEK code. The licence file is obtained from Data Encryption Systems, and the PEK code is entered by the user.

To begin the setup, the location of the licence file on the machine must be specified. Browse to the location of the file, or enter the location of the file directly. Click **Next** to continue.



DESlock+ DESkey Setup Wizard

Licence File

DESlock+ Software Edition requires a licence file.
If you already have one please enter its location below.

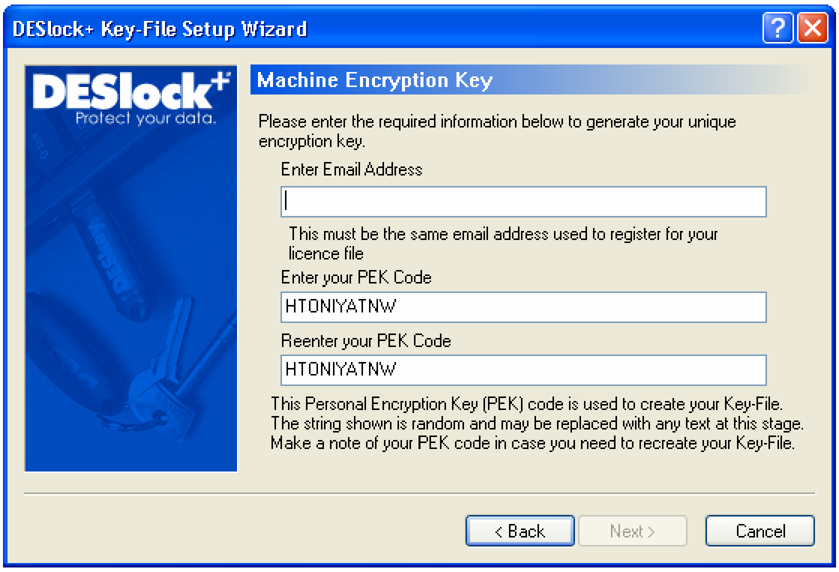
If you do not, you need access to the DESlock+ website and your email account.
Please click the link below to obtain a licence.

Obtain a licence file

Licence File

Figure 3 - 34

Next, enter the PEK code. The licence file and PEK code determine the encryption key the Key-File will provide. Any PEK code can be entered, although the encryption key cannot be recreated without knowing the PEK code so a note of it should be kept in a safe place as a backup.



Machine Encryption Key

Please enter the required information below to generate your unique encryption key.

Enter Email Address

This must be the same email address used to register for your licence file

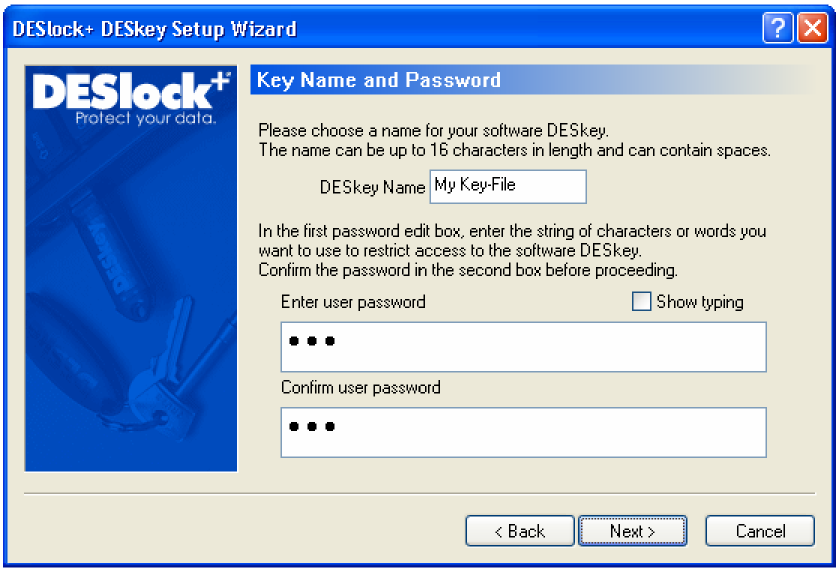
Enter your PEK Code: HTONIYATNW

Reenter your PEK Code: HTONIYATNW

This Personal Encryption Key (PEK) code is used to create your Key-File. The string shown is random and may be replaced with any text at this stage. Make a note of your PEK code in case you need to recreate your Key-File.

Figure 3 - 35

Next enter the name by which to refer to the Key-File and the password you require to secure access to the Key-File. If the password to the Key-File is lost, the Key-File can be recreated only if both the licence file and PEK code are known.



Key Name and Password

Please choose a name for your software DESkey.
The name can be up to 16 characters in length and can contain spaces.

DESkey Name: My Key-File

In the first password edit box, enter the string of characters or words you want to use to restrict access to the software DESkey.
Confirm the password in the second box before proceeding.

Enter user password ☐ Show typing

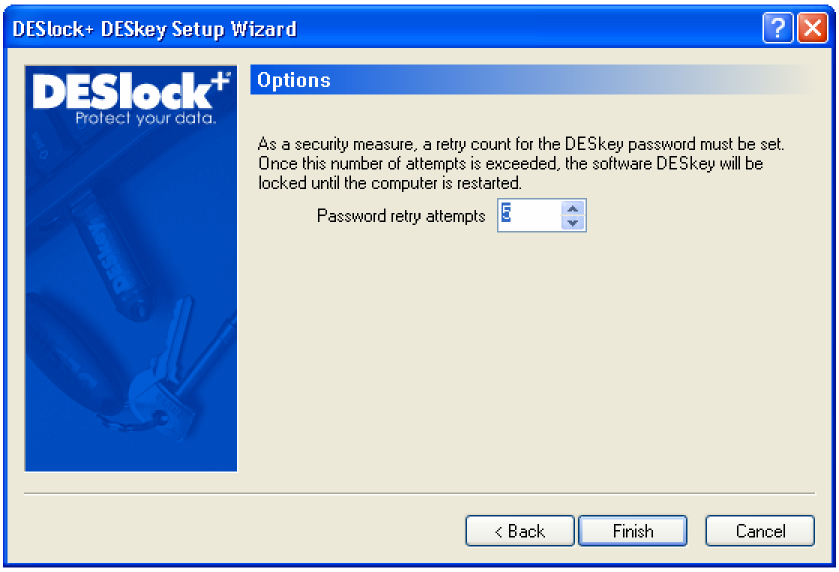
●●●

Confirm user password

●●●

Figure 3 - 36

Access to the Key-File is secured by the password entered. To deter against attempts at guessing this password, the Key-File will become disabled if an invalid password is entered too many times. The Key-File will only become active again after a complete reboot of the system, at which point the bad password counter will be reset. Set the number of password attempts here.



Options

As a security measure, a retry count for the DESkey password must be set. Once this number of attempts is exceeded, the software DESkey will be locked until the computer is restarted.

Password retry attempts 5

Figure 3 - 37

This page has been intentionally left blank

Activating DESlock⁺

Before use, DESlock⁺ may be in a disabled state, denoted by the flashing disabled state icon in the system tray (Figure 4 - 1).

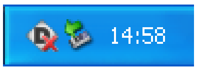


Figure 4 - 1

To activate DESlock⁺ you must login to an attached and already setup DK5 DESkey or software Key-File. If either is available, right click the DESlock⁺ icon and select **Activate** (Figure 4 - 2).

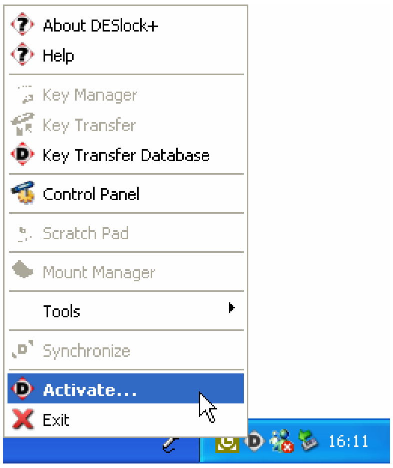
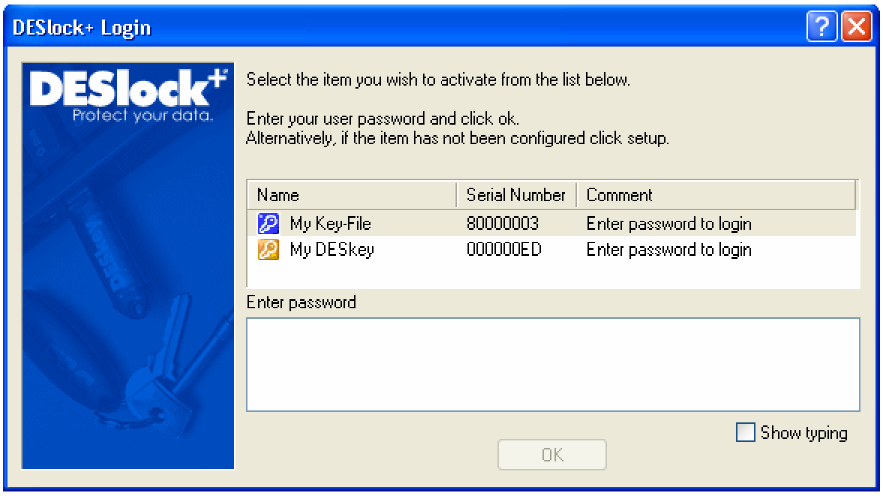


Figure 4 - 2

The **DESlock+ Login** box will now be displayed (Figure 4 - 3). Select the DESkey or Key-File you wish to activate and enter the correct user password for that DESkey and click OK. Click ✕ or press the Esc key to close the login box without logging in.



Select the item you wish to activate from the list below.

Enter your user password and click ok.
Alternatively, if the item has not been configured click setup.

Name	Serial Number	Comment
My Key-File	80000003	Enter password to login
My DESkey	000000ED	Enter password to login

Enter password

□ Show typing

OK

Figure 4 - 3

Check the **Perform Master Login** box and enter the correct Master password to login to a DK5 DESkey as a Master rather than a User. Click the **Show Typing** box to make the password visible on screen. This option is not available with Key-Files.

If the password was entered correctly, the DESlock$^+$ icon in the system tray will change to the enabled state (Figure 4 - 4) and DESlock$^+$ can now be used.

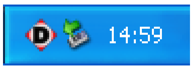


Figure 4 - 4

If the password was entered incorrectly, the user can reattempt to login.

The DESkey will be disabled after the configured number of wrong password attempts. The number of attempts allowed, plus a subsequent security measure, was defined during DESkey setup. This behaviour can be changed via the DESlock$^+$ Control Panel when logged in as a Master (see pages 49 and 52).

Using DESlock$^+$

When DESlock$^+$ is active, the system tray menu will change as shown below (Figure 4 - 5). Note that previously disabled menu items are now available and the 'Activate' entry has changed to 'Deactivate'.

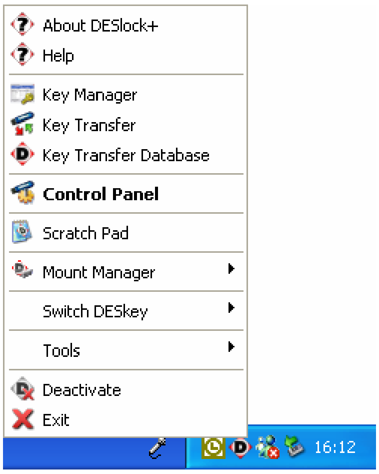
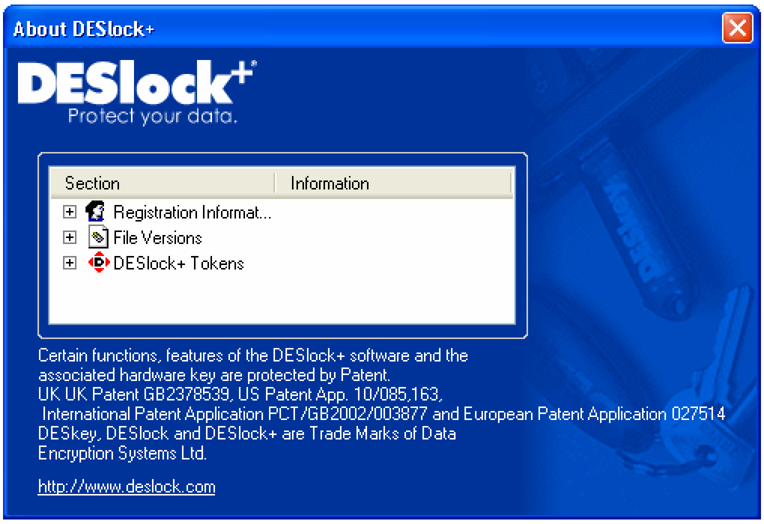


Figure 4 - 5

Menu Options

About DESlock+

The About Box will display product information.



Certain functions, features of the DESlock+ software and the associated hardware key are protected by Patent.
UK UK Patent GB2378539, US Patent App. 10/085,163,
International Patent Application PCT/GB2002/003877 and European Patent Application 027514
DESkey, DESlock and DESlock+ are Trade Marks of Data Encryption Systems Ltd.

http://www.deslock.com

Figure 4 - 6

Help

Brings up the help and documentation.

Key Manager

The Encryption Key Manager dialog allows the user to create, delete and manage encryption keys (see page 55).

Key Transfer

The Key Transfer Wizard allows encryption keys to be transferred between DK5 DESkeys (see page 69).

Key Transfer Database

The Key Transfer Database allows direct access to the key transfer database stored on this machine (see page 67).

Control Panel

This will launch the DESlock$^+$ Control Panel (see page 43).

Scratch Pad

Used to access a protected memory area within the DK5 DESkey which can be used to store sensitive information (see page 109).

Mount Manager

This will launch the DESlock$^+$ Mount Manager (see page 89).

Switch DESkey

If multiple DESkeys are inserted, an additional menu item will appear (Figure 4 - 7) so that the user can easily switch between them. The extra menu item will only be visible whilst multiple DK5 DESkeys are inserted and one of them has been activated.

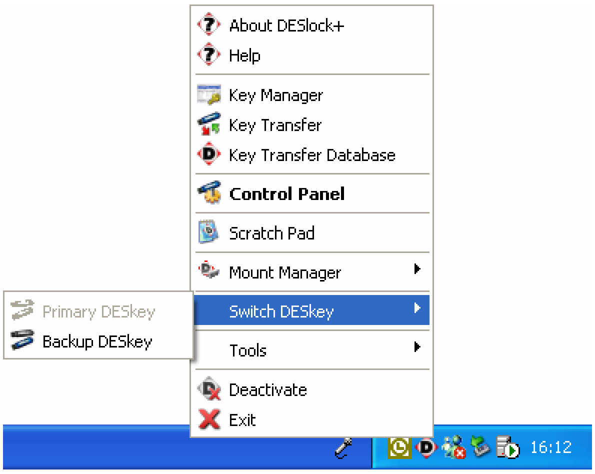


Figure 4 - 7

Switching DESkeys will automatically deactivate DESlock$^+$ and log out of the current active DESkey. The login box will then be shown so DESlock$^+$ can be reactivated with the selected DESkey.

The current active DESkey will be displayed in the list but will be greyed out and cannot be selected.

Tools

This will launch the DESlock$^+$ text encryption tools, as described on page 84.

Synchronize

Synchronises all offline folders. See page 86 for more details on offline folders.

Deactivate

Clicking deactivate, or simply removing the DESkey, will force DESlock$^+$ to deactivate itself. After Deactivation, DESlock$^+$ will remain running and can be reactivated later.

Exit

Clicking Exit will disable and close DESlock$^+$. This will unload DESlock$^+$ and remove the icon from the system tray.

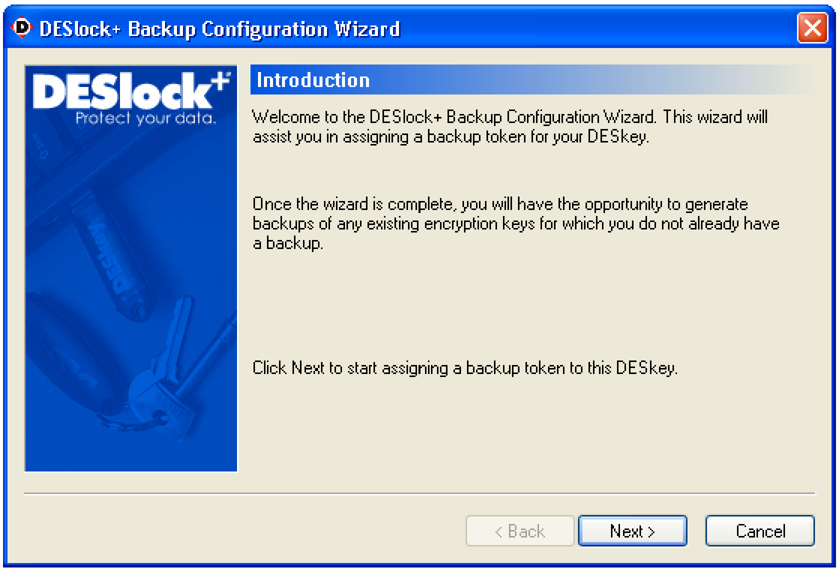
Backup Configuration Wizard

When a DK5 DESkey is configured initially, the backup assignments shown on the Backup Page of the DESlock$^+$ Control Panel (shown on page 50) will not have been set. Until at least one has been set, each time the DESkey is activated the following wizard will run.

This wizard enables the Backup DESkey assignments to be quickly made and any non-backed up encryption keys to be backed up.

The wizard may be cancelled, but it will run each time the DESkey is activated until at least one Backup assignment has been made.

This wizard will only appear when activating a DK5 DESkey and will never appear when activating a Key-File.



Welcome to the DESlock+ Backup Configuration Wizard. This wizard will assist you in assigning a backup token for your DESkey.

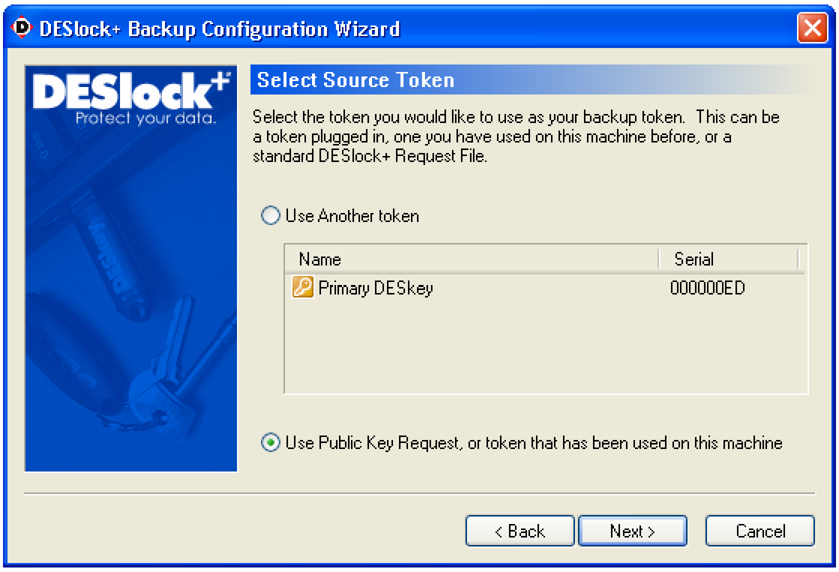
Once the wizard is complete, you will have the opportunity to generate backups of any existing encryption keys for which you do not already have a backup.

Click Next to start assigning a backup token to this DESkey.

Figure 5 - 1

The first step in the wizard is to specify the 'Backup DESkey'. The Backup DESkey can be any other DESkey, and should be set to the DESkey to which you will most commonly use to store copies of encryption keys.

The assignment can be made from another DESkey that is connected to the machine, or by using an entry from the Key Transfer Database (see page 67) or from a DESkey encryption key request file (dlr file). Refer to page 71 for information on creating encryption key request files.



Select Source Token

Select the token you would like to use as your backup token. This can be a token plugged in, one you have used on this machine before, or a standard DESlock+ Request File.

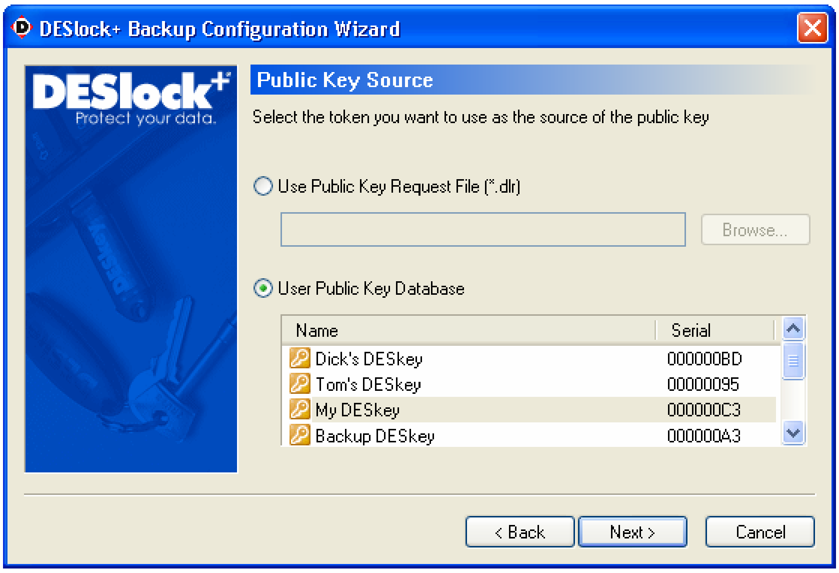
○ Use Another token

Name	Serial
Primary DESkey	000000ED

● Use Public Key Request, or token that has been used on this machine

Figure 5 - 2

If the 'Use Public Key Request…' option is chosen, one must then specify which key request to use, or which entry from the Key Transfer Database to use. All available entries in the Key Transfer Database will be listed, and the option to browse to a a DESkey encryption key request file (dlr file) is given.



Public Key Source

Select the token you want to use as the source of the public key

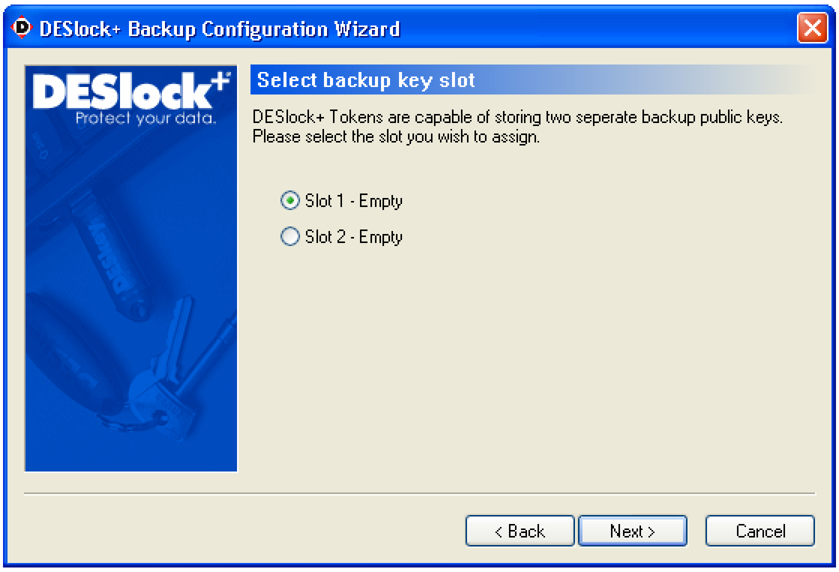
○ Use Public Key Request File (*.dlr)

● User Public Key Database

Name	Serial
Dick's DESkey	000000BD
Tom's DESkey	00000095
My DESkey	000000C3
Backup DESkey	000000A3

Figure 5 - 3

Next one of the two available assignment slots must be specified to be used. The DESkey selected previously will be added as the backup DESkey into the slot selected.



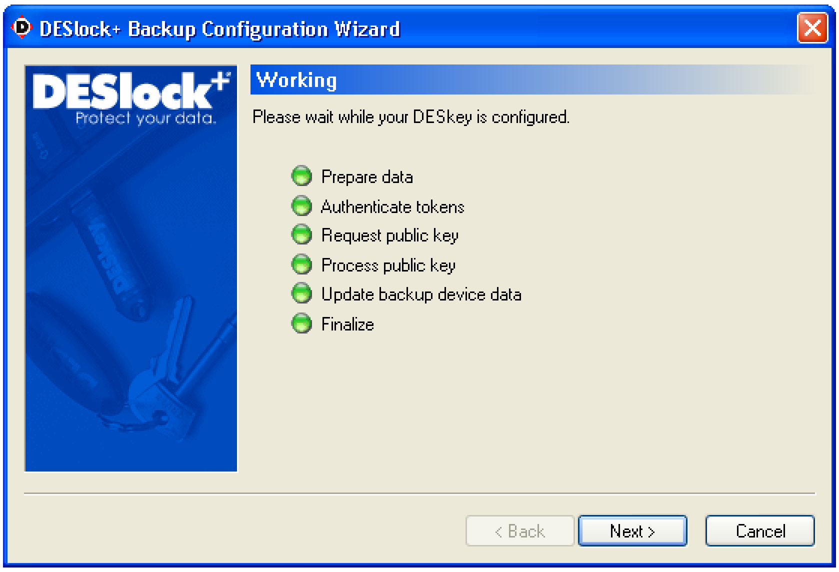
Select backup key slot

DESlock+ Tokens are capable of storing two seperate backup public keys.
Please select the slot you wish to assign.

● Slot 1 - Empty
○ Slot 2 - Empty

Figure 5 - 4

The wizard will then make the backup assignment.



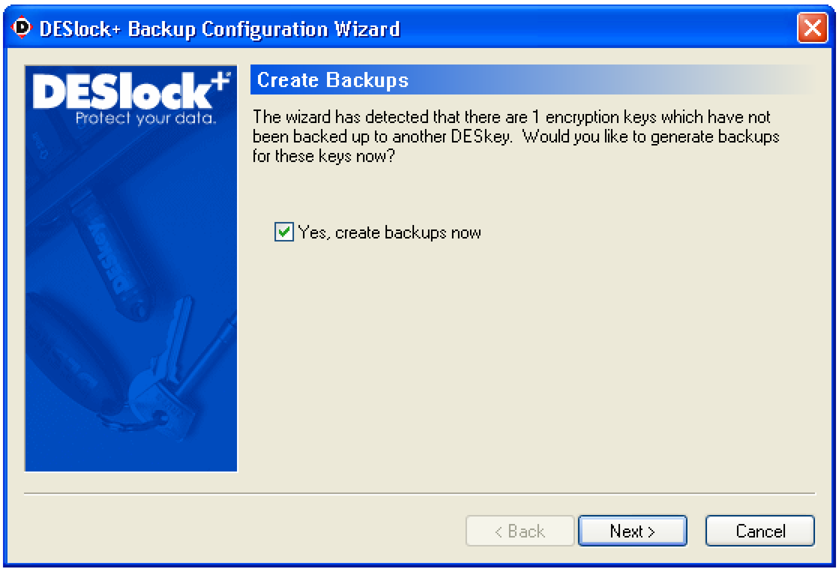
Working

Please wait while your DESkey is configured.

- Prepare data
- Authenticate tokens
- Request public key
- Process public key
- Update backup device data
- Finalize

Figure 5 - 5

If the current DESkey contains any encryption keys that have not yet been backed up, this wizard can extract them so they may be added to the previously specified Backup DESkey. Please note, only encryption keys that have *not* been backed up to another DESkey will be extracted, and the updates must be manually imported into the specified Backup DESkey following this extraction in order to complete the backup process.



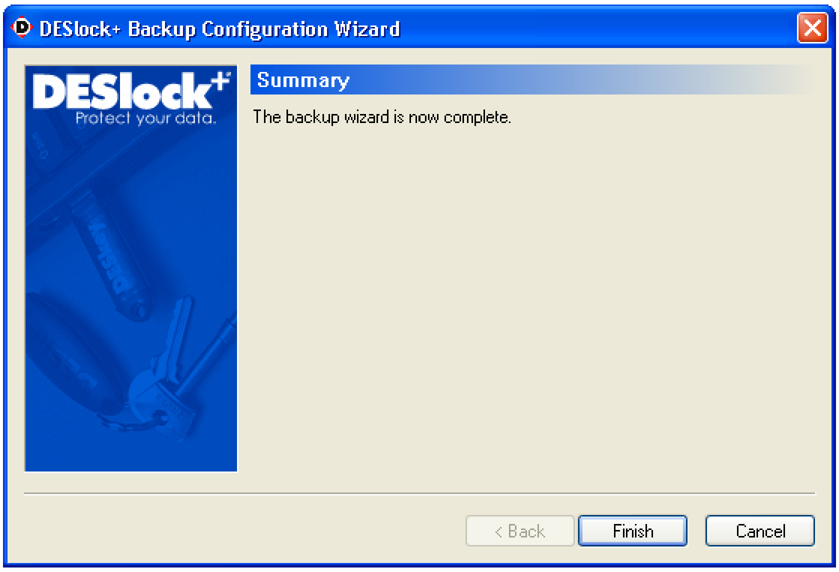
Create Backups

The wizard has detected that there are 1 encryption keys which have not been backed up to another DESkey. Would you like to generate backups for these keys now?

☑ Yes, create backups now

Figure 5 - 6

When the wizard is complete, the backup assignment in the DESkey will have been set and saved, and any un-backed up encryption keys found will have been extracted and can then be imported into the backup DESkey using the key manager restore function by using the Backup DESkey on this machine (see page 62).



Summary

The backup wizard is now complete.

Figure 5 - 7

Terminator and Group Codes

Description

The Terminator Code is a value within an encryption key to allow the originator control over the propagation of that encryption key. To transfer a key to another DESkey this value must be more than 0. When a key is transferred, the Terminator Code is decremented in the copy, but remains unchanged in the original.

The Group Code defines a group the DESkey can be a member of and can be used to further restrict key transfers. By default, a DESkey will not be members of any group and any encryption keys generated can, assuming a valid terminator code, be transferred to any other DESkey. However, if the DESkey is a member of a group, any encryption keys generated by that DESkey can be tied to the group so encryption keys cannot, even if the terminator code allows it, be transferred to another DESkey that is not in the same group. Even if the DESkey is a member of a group, it can still generate encryption keys that can be transferred to DESkeys outside of the group if required.

A DESkey can be a member of only one group at any one time. The group code must be set by Data Encryption Systems.

Terminator Code Example

In many cases when a common encryption key is transferred between users, the originator will want to decide whether or not a recipient can forward the key to another user.

Suppose User A creates a new project key and wishes to share it with others on the project team. User A sends the key to B and C with a Terminator Code of 0, to User D with a code of 1 and to User E with a code of 2.

Users B and C cannot copy the key any further.

User D can copy the key to other users, in this case F and G.

Because the Terminator Code is decremented at every generation, users F and G cannot copy the key.

User E had a value of 2, who copied the key to user H who in turn copied it to I, J and K.

I, J and K cannot copy the key any further.

User E also copied it to User L but in this instance manually reduced the Terminator Code to 0 (it cannot be increased or kept constant.)

L is unable to copy the key any further.

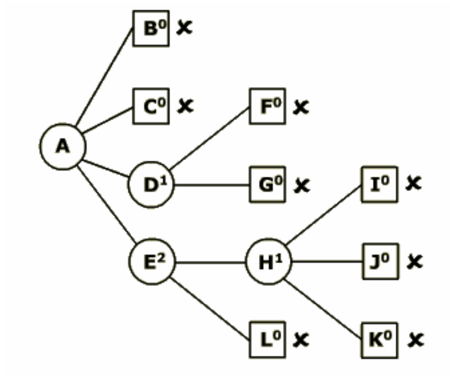


Figure 6 - 1

Group Code Example

To maintain data security, it is often necessary to control key transfers within a defined group.

In this example, user A creates a new project key and wishes to share it with others on the project team. Group code has been assigned to match that of User A’s DESkey.

User A has previously issued B, C, D and E with DESkey units having the correct fixed Group Code. User F is not a project team member and does not have a correctly coded DESkey unit.

User A transfers the key to B, with a terminator code of 1. B is then left to update the other users. C, D and E are successfully updated, but F cannot receive the encryption key.

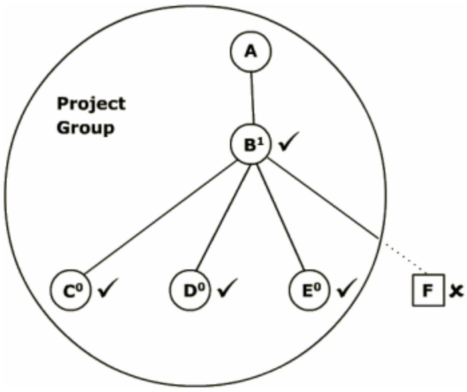


Figure 6 - 2

DESlock$^+$ Control Panel

The DESlock$^+$ Control Panel allows the user to configure the DESlock$^+$ program and to set various DESkey options. It can be launched by double clicking on the DESlock$^+$ icon (Figure 7 - 1) in the Windows Control Panel or from the DESlock$^+$ system tray icon. Some control panel pages are dependant on the activated status of DESlock$^+$ and may not be available at all times.

Figure 7 - 1

If running under Windows XP you may need to turn 'Classic View' on to see the control panel icon in Windows control panel. Note that the control panel menu item will always be present on the DESlock$^+$ system tray menu even if it is not visible in the Windows control panel.

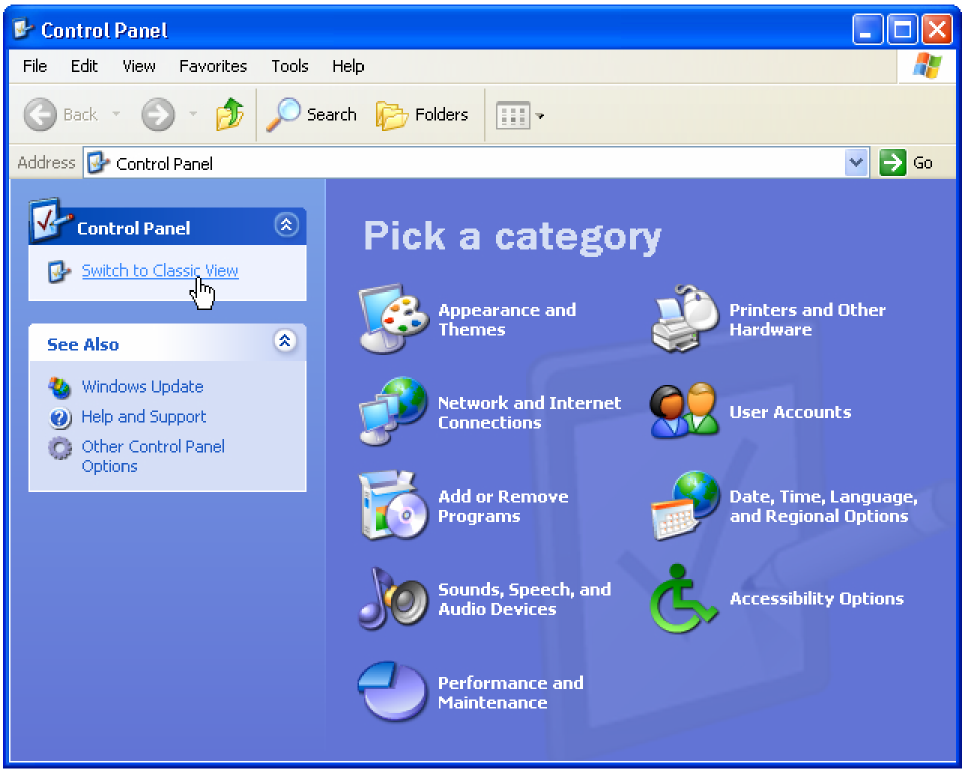
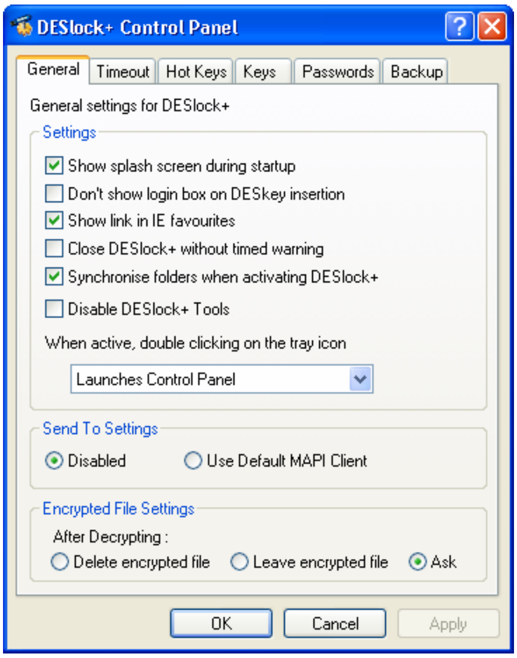


Figure 7 - 2

General

The general page allows the DESlock^{+} options to be modified.


DESlock+ Control Panel

General settings for DESlock+

Settings

☑ Show splash screen during startup
□ Don't show login box on DESkey insertion
☑ Show link in IE favourites
□ Close DESlock+ without timed warning
☑ Synchronise folders when activating DESlock+
□ Disable DESlock+ Tools

When active, double clicking on the tray icon: Launches Control Panel

Send To Settings

● Disabled ○ Use Default MAPI Client

Encrypted File Settings

After Decrypting :
○ Delete encrypted file ○ Leave encrypted file ● Ask

Figure 7 - 3

Settings

Show splash screen during startup

Select to show a splash screen when DESlock^{+} is loading.

Don't show login box on DESkey insertion

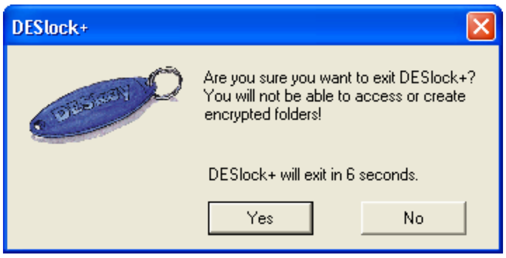
Select to not show the login box when a DESkey is inserted.

Show link in IE Favourites

If selected, a URL to the DESlock^{+} website will be placed in the Internet Explorer favourites list.

Close DESlock+ without timed warning

If this option not selected, a warning box (Figure 7 - 4) will be displayed if DESlock^{+} is activated and the user attempts to exit the application. The shutdown can be cancelled before the 10 second timout is complete.


DESlock+

Are you sure you want to exit DESlock+? You will not be able to access or create encrypted folders!

DESlock+ will exit in 6 seconds.

Figure 7 - 4

Synchronise folders when activating DESlock+

If selected, any DESlock+ offline network folders will attempt to be synchronised with the local copy. See page 86 for more details on DESlock+ offline folders.

Disable DESlock+ Tools

If selected, DESlock+ Tools will be disabled and will not be available for use in any application.

When active, double clicking on the tray icon:

Choose the desired double click option from the drop down list. This relates to the action performed when double clicking on the icon in the system tray.

Send to settings

Disabled

Do not allow an encryption key to be emailed directly from the key manager using the "Send To…" option.

Use Default MAPI client

Use the default MAPI client to allow encryption keys to be emailed using the standard Windows "Send To…" shell extension option.

Encrypted file settings

Delete encrypted file

If selected, when decrypting an individual file (see page 82) the encrypted original copy will be deleted.

Leave encrypted file

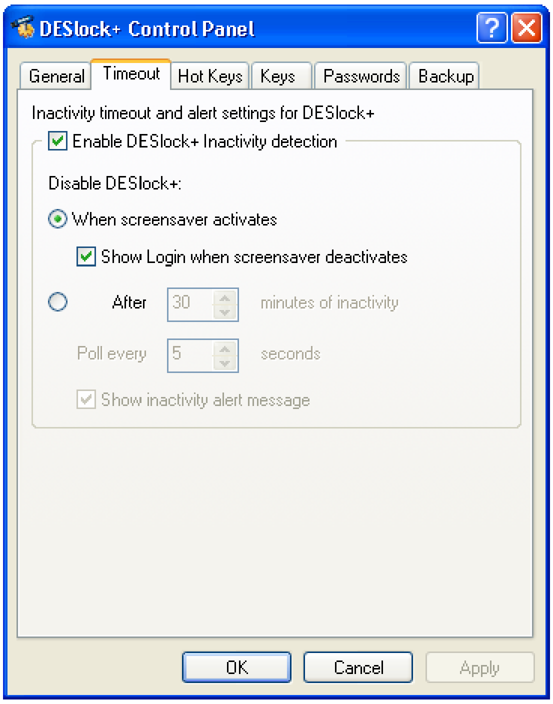
If selected, when decrypting an individual file (see page 82) the encrypted original copy will be left.

Ask

If selected, when decrypting an individual file (see page 82) the user will be prompted to choose what to do with the encrypted original copy.

Timeout

The Timeout options control the inactivity timeout detection of DESlock$^+$.


DESlock+ Control Panel

Inactivity timeout and alert settings for DESlock+

☑ Enable DESlock+ Inactivity detection

Disable DESlock+:

● When screensaver activates

☑ Show Login when screensaver deactivates

○ After 30 minutes of inactivity

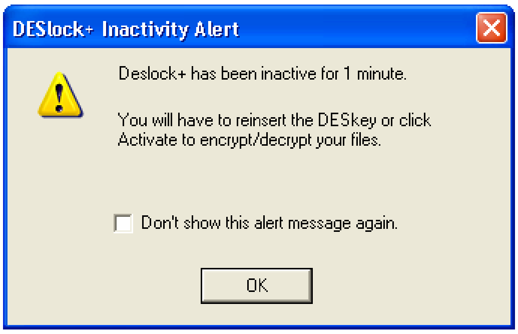
Poll every 5 seconds

☑ Show inactivity alert message

Figure 7 - 5

When enabled, DESlock$^+$ can deactivate itself after a period of inactivity. This is measured as the idle time since the last key press or mouse movement, whichever is later. Alternatively, DESlock+ can be automatically deactivated when the Windows screensaver is activated.

The 'Show inactivity alert message' controls whether a warning dialog box (Figure 7 - 6) will be displayed when DESlock$^+$ has been deactivated due to inactivity.


DESlock+ Inactivity Alert

Deslock+ has been inactive for 1 minute.

You will have to reinsert the DESkey or click Activate to encrypt/decrypt your files.

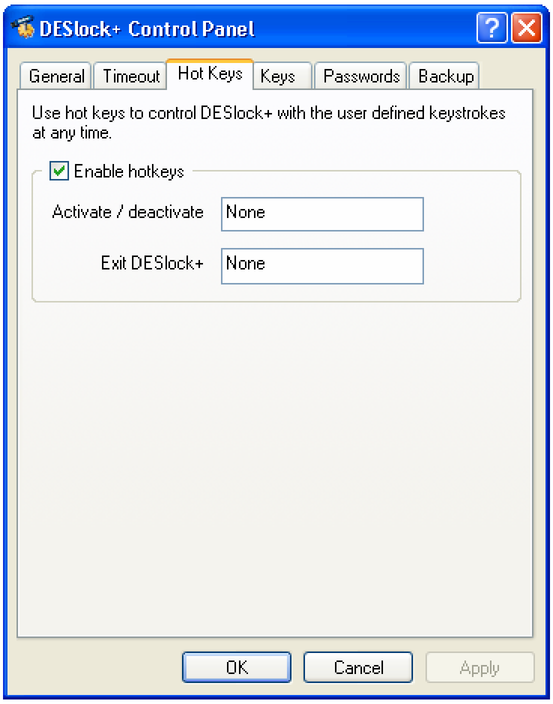
□ Don't show this alert message again.

Figure 7 - 6

Once deactivated, access to protected files will be denied and the user must log back into the DESkey to continue working with protected files.

Hot Keys

Hot keys are keyboard shortcuts that can be used to quickly activate a particular function.



Use hot keys to control DESlock+ with the user defined keystrokes at any time.

☑ Enable hotkeys

Activate / deactivate: None

Exit DESlock+: None

Figure 7 - 7

Two hot keys are available in DESlock$^+$ to close DESlock$^+$ and remove it from the system tray or to control activation of the DESkey: If the DESkey is currently active the hot key will deactivate it; If the DESkey is not active the hot key will activate it and prompt the user to login.

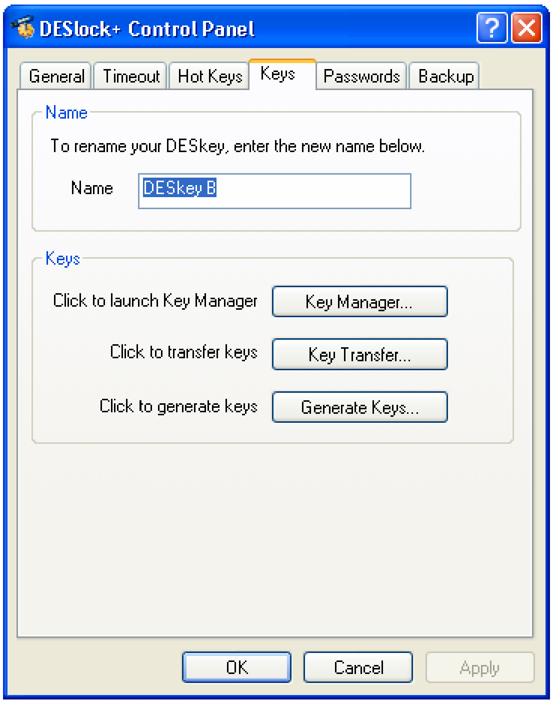
To enable these options make sure the check box is set and type the desired key press combination into the edit box. The result will then automatically be displayed. If the value needs to be modified, simply type the new key press combination and it will be automatically updated.

Use the 'Space' key to clear the hot key selection.

Keys

The options available on the Keys page are dependent on user privileges so this may require being logged on as a Master. It allows access to the encryption key wizards and allows the DESkey name to be changed.

This page is only available if DESlock$^+$ has been activated with a DK5 DESkey.



To rename your DESkey, enter the new name below.

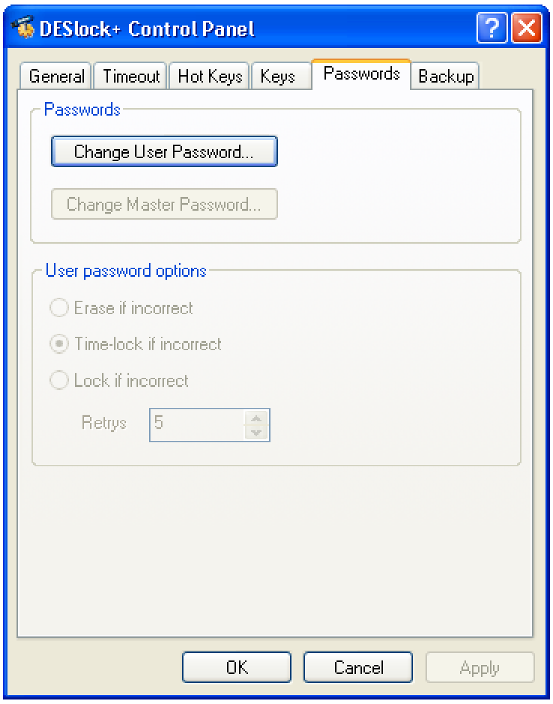
Name: DESkey B

Figure 7 - 8

Passwords

The options available on the Passwords page are dependent on user privileges so this may require being logged on as a Master. It allows the user and master password to be changed along with the user password retry limit and resulting action to be modified.

This page is only available if DESlock^{+} has been activated with a DK5 DESkey.



Passwords

User password options

○ Erase if incorrect

● Time-lock if incorrect

○ Lock if incorrect

Retrys 5

Figure 7 - 9

User Password Options

Erase if incorrect: If selected, all encryption keys held within the DESkey will be deleted.

Time-loop if incorrect: If selected, the DESkey will enter a time loop delay between login attempts. The time delay will increase exponentially starting at 1 minute.

Lock if incorrect: This option is only available for the user account. If selected the DESkey will only respond when logging in as a master, even if the correct user password is used. Successfully logging in as a master will unlock the user account.

Retries: This specifies the number of consecutive wrong password attempts the DESkey will permit before performing the specified action.

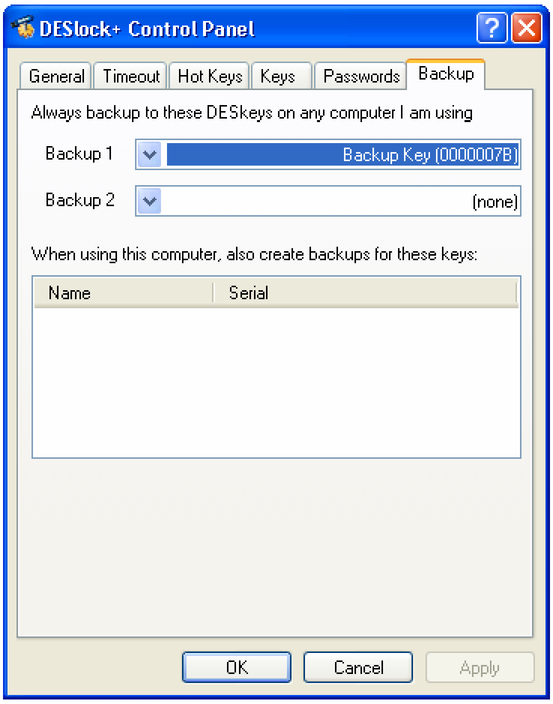
Backup

Backup assignments

Backup DESkeys are intended to store copies of important encryption keys so that encrypted data can still be accessed even if the original DESkey and/or encryption key is lost. **If the only copy of an encryption key is lost there is no way to recover data encrypted using the key, so important keys should always be backed up**.

Each DESkey can store details of two other DESkeys which can be assigned as intended recipients for encryption key backups. The Backup page is used to assign the Backup DESkeys.

This page is only available if DESlock+ has been activated with a DK5 DESkey.



Always backup to these DESkeys on any computer I am using

Backup 1: Backup Key (0000007B)

Backup 2: (none)

When using this computer, also create backups for these keys:

Name	Serial

Figure 7 - 10

Backup DESkeys can only be assigned from the local Key Transfer Database. This means to be present in the local Key Transfer Database either the DESkey must have been setup on the local machine or the public key must have been imported when the key transfer wizard was used previously.

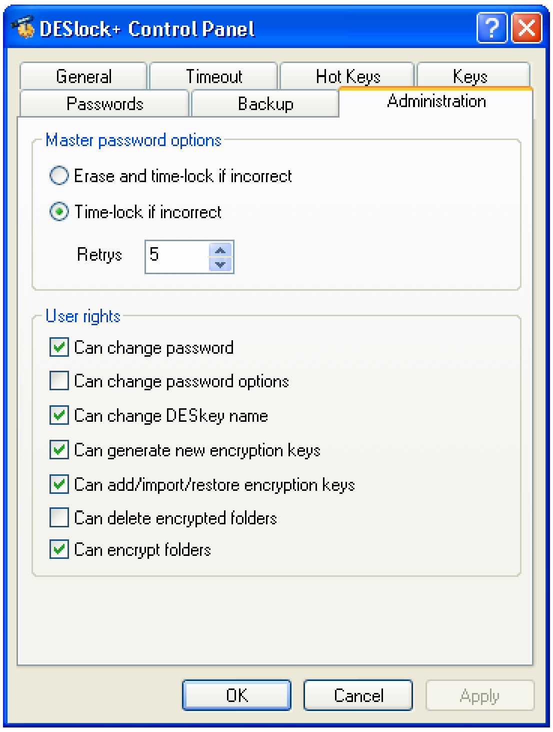
The benefit of the two Backup assignments is that the details are stored in the hardware of the DESkey itself. This means that encryption key backups can be created for these two DESkeys on any machine, regardless of whether or not the local Key Transfer Database also has details of the DESkeys.

Encryption keys can be Backed up either when they are created using the Key Generation Wizard, or by using the Encryption Key Manager. Encryption keys may also be transferred to a backup DESkey using the Key Transfer Wizard. The backup process is described in more detail in the Key Manager section of the manual.

If DESlock$^+$ is activated but no Backup DESkey assignments have been made in the active DESkey, the Backup Configuration Wizard will run. This is described on page 31.

Administration

The Administration page is only available when logged into a DK5 DESkey with the Master password. It allows DESkey options to be set.



Master password options

○ Erase and time-lock if incorrect

● Time-lock if incorrect

Retrys 5

User rights

☑ Can change password

□ Can change password options

☑ Can change DESkey name

☑ Can generate new encryption keys

☑ Can add/import/restore encryption keys

□ Can delete encrypted folders

☑ Can encrypt folders

Figure 7 - 11

Master Password Options

These options will control the action in the event of the specified number of consecutive incorrect password attempts being entered in an attempt to login.

Erase and time-lock if incorrect: If selected, all encryption keys held within the DESkey will be deleted. This will also enable the time-lock feature.

Time-lock if incorrect: If selected, the DESkey will enter a time loop delay between login attempts. The time delay will increase exponentially starting at 1 minute.

Retries: This specifies the number of consecutive wrong password attempts the DESkey will permit before performing the specified action.

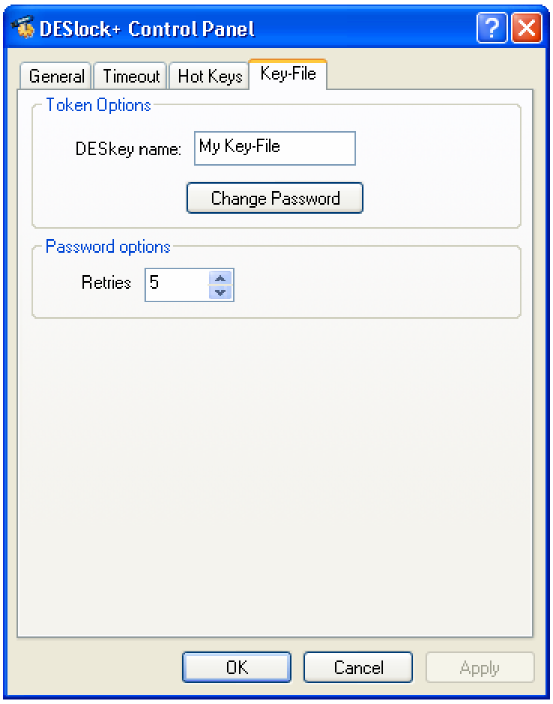
User Rights

Select the operations that are available when logged on as a User. Please note that when logged in with the master password there are no access restrictions.

Key-File

The Key-File page allows the Key-File name, password and password retries count to be configured. If the incorrect password is entered more than the retries count, the Key-File will be disabled until the machine has been rebooted.

This page is only available when DESlock$^+$ has been activated with a Key-File.



DESkey name: My Key-File

Retries 5

Figure 7 - 12

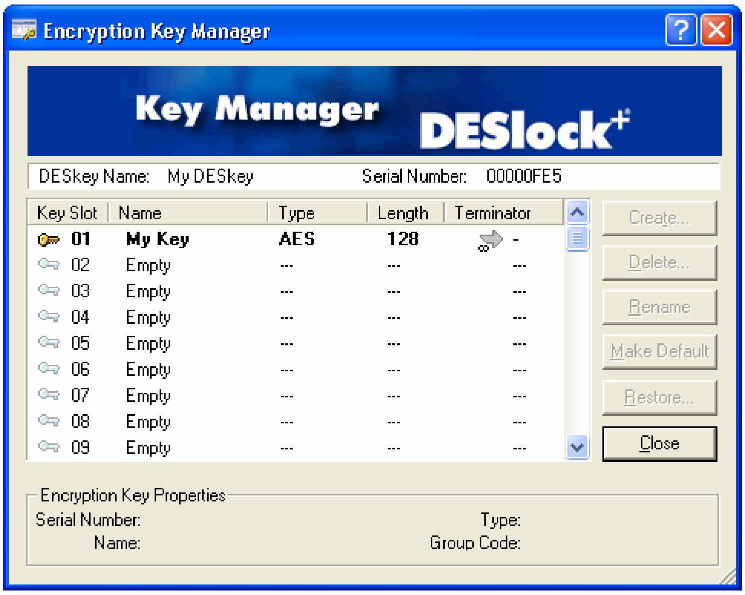
This page has been intentionally left blank

Encryption Key Manager

The Encryption Key Manager allows encryption keys to be created, renamed, deleted, transferred, backed up and restored.

The Encryption Key Manager can be launched by right clicking the DESlock$^+$ icon in the system tray and selecting **Key Manager**.

When using DESlock$^+$ with a Key-File, this applet is for reference only as there is no encryption key management functionality with a Key-File.



DESkey Name: My DESkey Serial Number: 00000FE5

Key Slot	Name	Type	Length	Terminator
01	**My Key**	**AES**	**128**	-
02	Empty	---	---	---
03	Empty	---	---	---
04	Empty	---	---	---
05	Empty	---	---	---
06	Empty	---	---	---
07	Empty	---	---	---
08	Empty	---	---	---
09	Empty	---	---	---

Encryption Key Properties

Serial Number: Type:

Name: Group Code:

Figure 8 - 1

The DESkey name and DESkey serial number are shown on this screen. The name can be changed at this stage if the logged in user has sufficient privileges to do so. The DESkey serial number cannot be changed and is shown for reference purposes only.

If the DESkey is a member of a key group (see page 41) then the group code will be shown to the right of the serial number. If the DESkey is not a member of a group then nothing will be shown.

Key Storage

All encryption keys are stored within the DESkey. The list shown above is split into multiple rows representing the 64 key slots available. The columns are labelled as follows:

Key Slot

The location of the encryption key in the DESkey key storage space.

The following icons can be displayed alongside the slot number:

Icon	Meaning
🔑	The slot contains the default encryption key. Note the text will also be bold.
🔑	The slot contains an encryption key but it is not set as the default key.
🔑	The slot does not currently contain an encryption key.
!🔑 !🔑	The slot contains an encryption key (which may be the default encryption key) but there is no record that a backup file or database entry has been made for any DESkey other than that which created the DESkey. If the DESkey is lost then any data encrypted using this key may be unrecoverable.

Name

A user definable descriptive name given to the encryption key. For example this could be the name of a person, a department or a project.

Type

The name of the algorithm the key can be used with. The various algorithm types available are AES (Rijndael), 3DES (Triple DES) and Blowfish. These are described in detail on page 2.

Length

The length of the key measured in bits. AES and Blowfish keys are 128-bits long. The 3DES key is 112-bits and comprises 2 unique 56-bit DES keys. Key length cannot be changed for these algorithms.

Terminator Code

The current value of the Terminator Code. Use of the terminator code is described in detail on page 41.

The following icons can be displayed to represent the terminator status.

Icon	Meaning
➔ 5	The Terminator Code value of this key is set to 5. This key can be transferred with a new Terminator Code value less than the value displayed i.e. the value can be no greater than 4.
✖ 0	The Terminator Code value of this key is zero. This key cannot be transferred under any circumstances.

The default terminator value for new keys is 255.

When issuing an encryption key, the Terminator Code of the original key will not change. The new value specifies the Terminator Code value of the encryption key within the destination DESkey.

Options

A list of option buttons is displayed on the right hand edge of the Encryption Key Manager. The options available are related to the state of the currently selected key slot e.g. the option to delete an empty key slot is not available.

These options can also be selected from a popup menu after right clicking anywhere within the key slot. Please note that some of these options are dependent on user permissions and may require Master access to perform them.

The following options may be available on a key slot containing an encryption key:

Delete Key

If selected, the encryption key will be deleted from the DESkey. A copy will be stored in the Key Transfer Database in case it needs to be imported at a later date.

If the only copy of an encryption key is lost there is no way to recover data encrypted using this key. Important keys should be backed up to avoid loss of data.

Rename

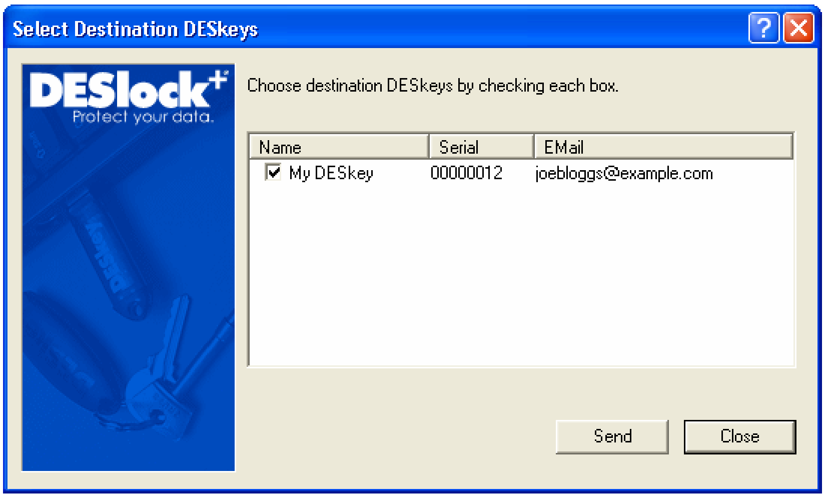
Renaming a key allows the descriptive name given to an encryption key to be changed.

Make Default

If the currently selected key is not the default, it can be made the default using this option. The default encryption key will always be highlighted and selected in the encryption key selection dialog box, when performing encryption.

Send To

This option is only available from the popup menu and allows an encryption key to be emailed to a DESkey defined in the Key Transfer Database. This option is only available if the option has been configured in the DESkey control panel (described on page 44). It is also only available for keys with a non-zero Terminator Code (described on page 41). The email address can be set in this dialog and once set will be saved.



Select Destination DESkeys

Choose destination DESkeys by checking each box.

Name	Serial	EMail
☑ My DESkey	00000012	joebloggs@example.com

Figure 8 - 2

The encryption key will be saved to a DESkey Update (DLU) file and emailed to the specified email address. The recipient of the email can then import the encryption key using the Key Transfer Wizard (described on page 69).

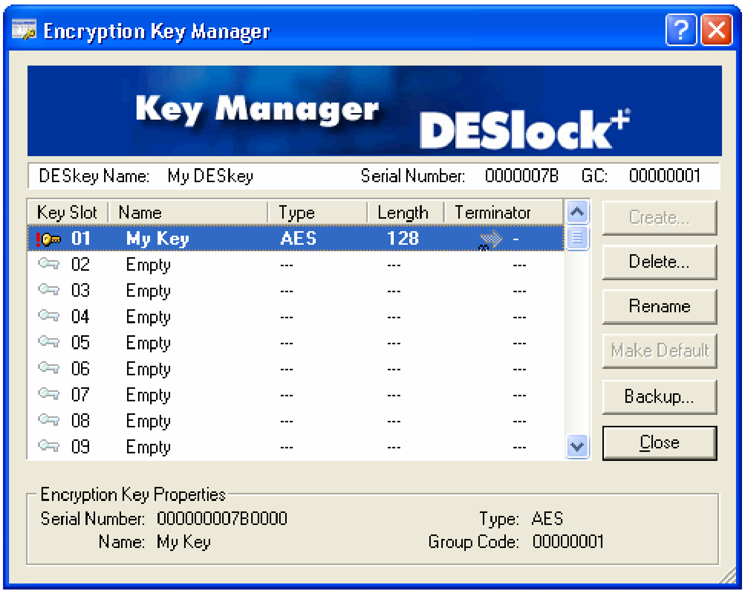
Backup

This will allow any encryption key, with a non-zero Terminator Code, to be backed up.

To backup an encryption key, it must be transferred to another DESkey. The backup process is two-fold. First you must extract the encryption key, and then you must import it into the destination DESkey. The encryption key cannot be extracted directly, instead one must specify the DESkey to which the encryption key is destined. This is done when the key is extracted, and the extracted key can then only be imported into the specified DESkey.

Only after the encryption key has been added to another DESkey's key space has the key actually been backed up to the other DESkey.

To extract the encryption key, open the Key Manager, select the key and click 'Backup'.



DESkey Name: My DESkey Serial Number: 0000007B GC: 00000001

Key Slot	Name	Type	Length	Terminator
01	My Key	AES	128	-
02	Empty	---	---	---
03	Empty	---	---	---
04	Empty	---	---	---
05	Empty	---	---	---
06	Empty	---	---	---
07	Empty	---	---	---
08	Empty	---	---	---
09	Empty	---	---	---

Encryption Key Properties
Serial Number: 000000007B0000 Type: AES
Name: My Key Group Code: 00000001

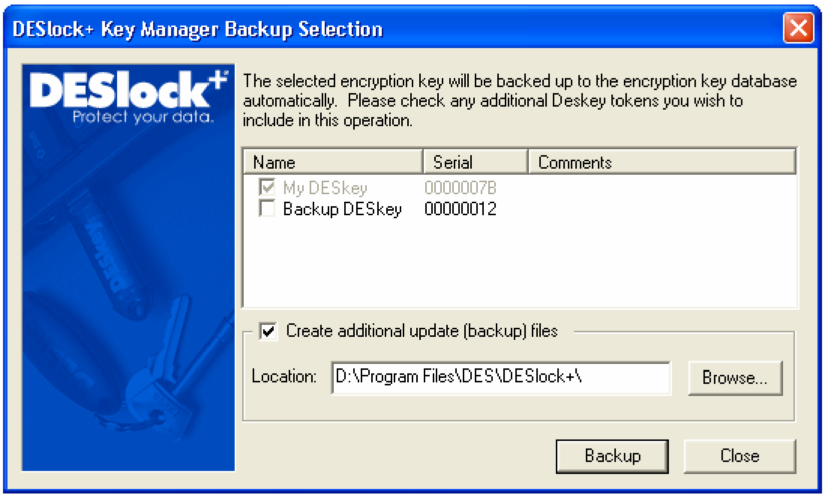
Figure 8 - 3

From this list, you must check all of the DESkeys to which you would like to backup the encryption key. Creation of a backup for itself is mandatory so the current DESkey will always be listed and cannot be deselected. As will any of the DESkeys added as backup assignments in the control panel (see page 50 of the DESlock$^+$ User Manual for information on making these assignments). Select any additional DESkeys you require from the list. Make sure the Backup DESkey is checked.

The list of available DESkeys is drawn from a database stored on the local machine. This database is described further on page 67.

If you wish to create backup files, which can be used on another machine, select the option and specify the folder to save the files into. These DESkey Update Files (DLU files) allow the encryption key to be imported using the Key Transfer Wizard. Refer the Key Transfer wizard update documentation, page 75 of the DESlock$^+$ User Manual, for more information on importing encryption keys this way.

e.g. in this case it will create a folder called "My DESkey (0000007B)" and in that folder it will create a file called "My Key.dlu". If 'Backup DESkey' was selected then it would create another folder called "Backup DESkey (00000012)" in which it would store another file called "My Key.dlu".



The selected encryption key will be backed up to the encryption key database automatically. Please check any additional Deskey tokens you wish to include in this operation.

Name	Serial	Comments
☑ My DESkey	0000007B	
□ Backup DESkey	00000012	

☑ Create additional update (backup) files

Location: D:\Program Files\DES\DESlock+\

Figure 8 - 4

Once the encryption key has been extracted, it must be imported into the destination DESkey to complete the backup process.

To do this, login to the destination/backup DESkey and re-open the key manager. Select an empty key slot and click the **Restore** button and select the encryption you wish to import.

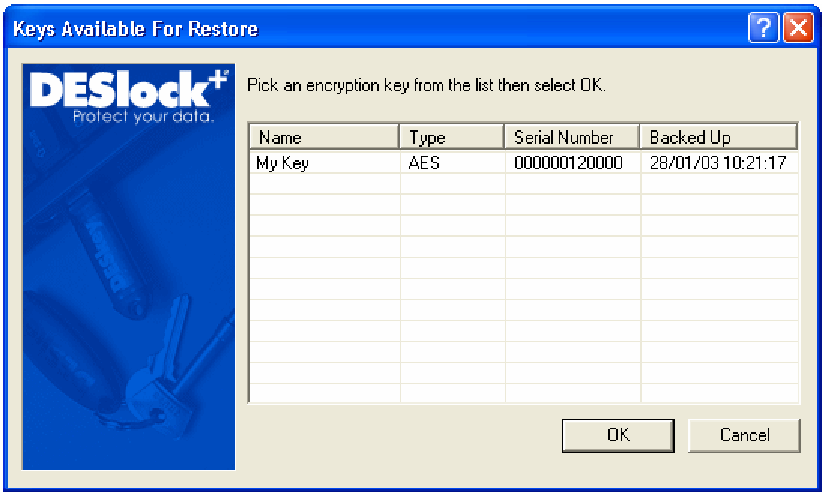
The following options may be available on an empty key slot:

Generate

This will launch the Key Generation Wizard in order to create a new key. This process is described on page 63.

Restore

This will allow previously deleted keys to be restored from the Key Transfer Database. Selecting this option will prompt the user to select a key to restore (Figure 8 - 5).



Pick an encryption key from the list then select OK.

Name	Type	Serial Number	Backed Up
My Key	AES	000000120000	28/01/03 10:21:17

Figure 8 - 5

Please note that this list may not contain all of the encryption keys stored in the Key Transfer Database. Only encryption keys that can be restored to the currently active DESkey will be displayed.

Once an encryption key has been selected and an empty key slot has been chosen, the key will be restored.

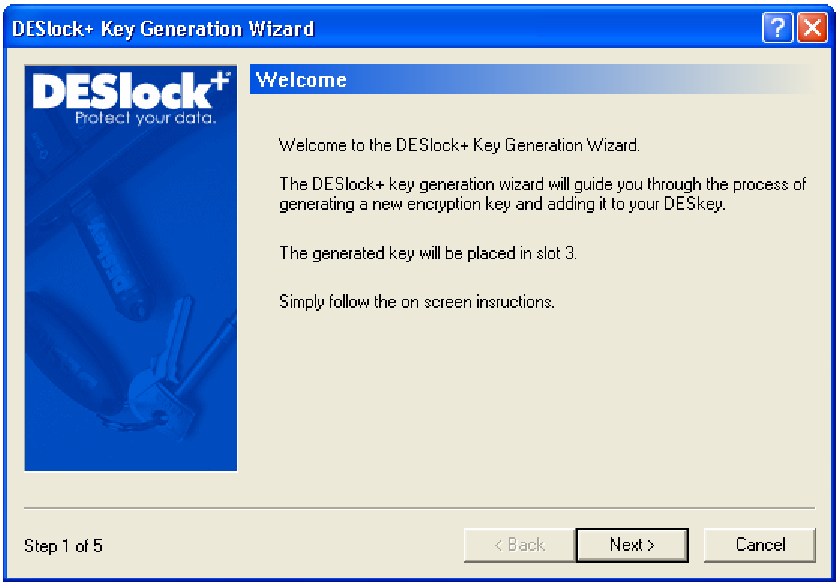
To restore an encryption key from a file rather than the local Key Transfer Database use the update option of the Key Transfer Wizard as described on page 75.

Key Generation Wizard

The Key Generation Wizard is used to create new encryption keys on a DK5 DESkey. New keys can be used to encrypt data and can also be transferred to other DK5 DESkeys if desired. Additional encryption keys cannot be created on a DESlock+ Key-File.

Generating a new Encryption Key

When the wizard is launched, the welcome screen (Figure 9 - 1) is shown. Click **Next** to begin key generation.



Welcome to the DESlock+ Key Generation Wizard.

The DESlock+ key generation wizard will guide you through the process of generating a new encryption key and adding it to your DESkey.

The generated key will be placed in slot 3.

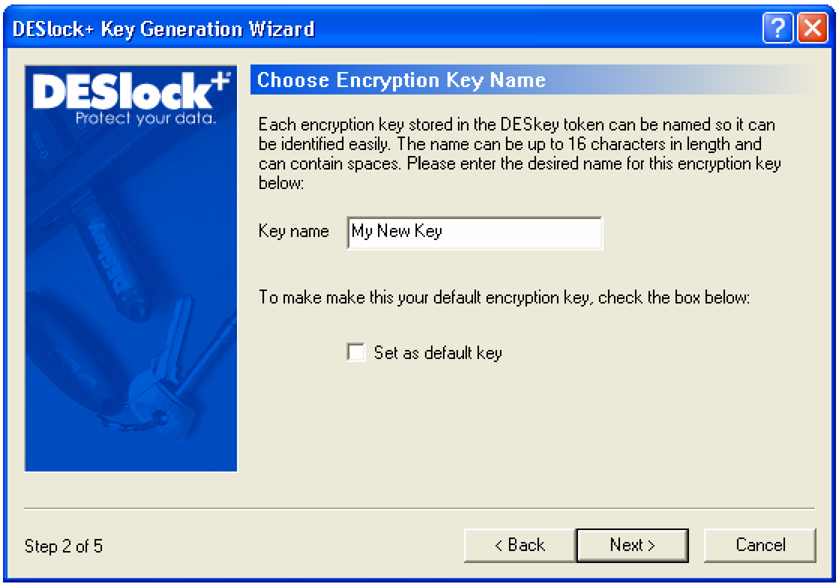
Simply follow the on screen insructions.

Step 1 of 5

Figure 9 - 1

Enter a name to identify the encryption key. This name can be anything for example the name of a person or the name of a project with which the key will be used.

The **Set as default key** checkbox is used to set this key as the default key for encryption. The default key will always be initially highlighted when selecting encryption keys. Click **Next** to continue.



DESlock+ Key Generation Wizard

Choose Encryption Key Name

Each encryption key stored in the DESkey token can be named so it can be identified easily. The name can be up to 16 characters in length and can contain spaces. Please enter the desired name for this encryption key below:

Key name: My New Key

To make make this your default encryption key, check the box below:

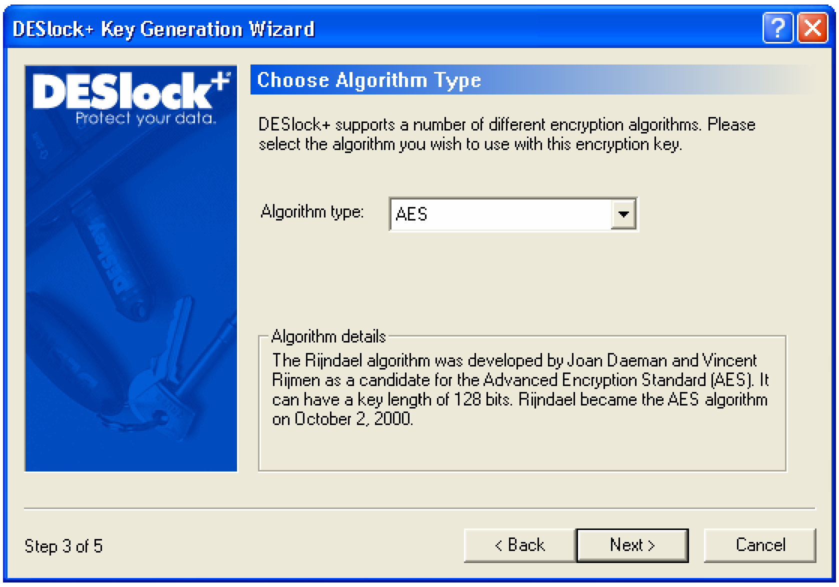
□ Set as default key

Step 2 of 5

Figure 9 - 2

Select the type of encryption key to generate. This relates to the algorithm that the key will be used with.

The different types of algorithm are described in more detail on page 2. A brief description is also given in the Algorithm Details box. Click **Next**.



DESlock+ Key Generation Wizard

Choose Algorithm Type

DESlock+ supports a number of different encryption algorithms. Please select the algorithm you wish to use with this encryption key.

Algorithm type: AES

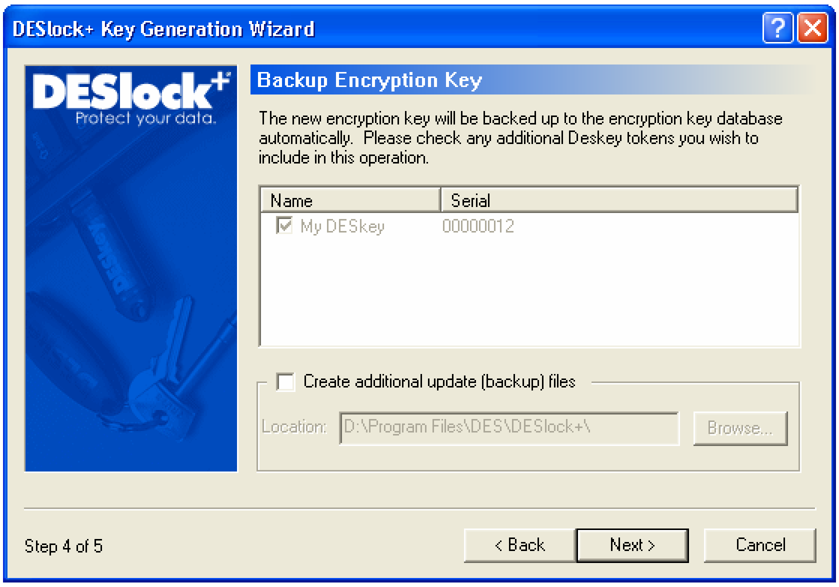
Algorithm details

The Rijndael algorithm was developed by Joan Daeman and Vincent Rijmen as a candidate for the Advanced Encryption Standard (AES). It can have a key length of 128 bits. Rijndael became the AES algorithm on October 2, 2000.

Step 3 of 5

Figure 9 - 3

If you choose to backup an encryption key, a copy will be saved to the Key Transfer Database (see page 67) and optionally also to a DESkey Update file. Saving to a file allows the encryption key to be imported to another DESkey using the Key Transfer Wizard (described on page 69).



The new encryption key will be backed up to the encryption key database automatically. Please check any additional Deskey tokens you wish to include in this operation.

Name	Serial
☑ My DESkey	00000012

□ Create additional update (backup) files

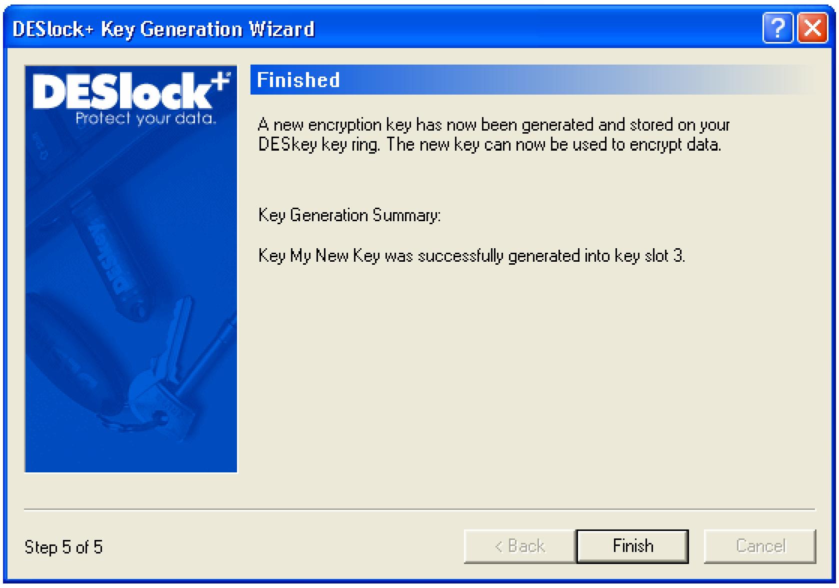
Location: D:\Program Files\DES\DESlock+\

Figure 9 - 4

From the target DESkey list, choose the DESkey(s) to which you wish the encryption key to be backed up. The list will contain any DESkey which is referenced in the Key Transfer Database on the local machine, or which is defined as a Backup key for the current DESkey (described on page 50).

See page 60 for more details on creating the backup file or database entry and information and additional steps required to complete the backup.

The new key has now been generated and added to the DESkey key space. It can now be used for encryption of data. The terminator code value of all new keys will be 255. Click Finish to end the Wizard.



A new encryption key has now been generated and stored on your DESkey key ring. The new key can now be used to encrypt data.

Key Generation Summary:

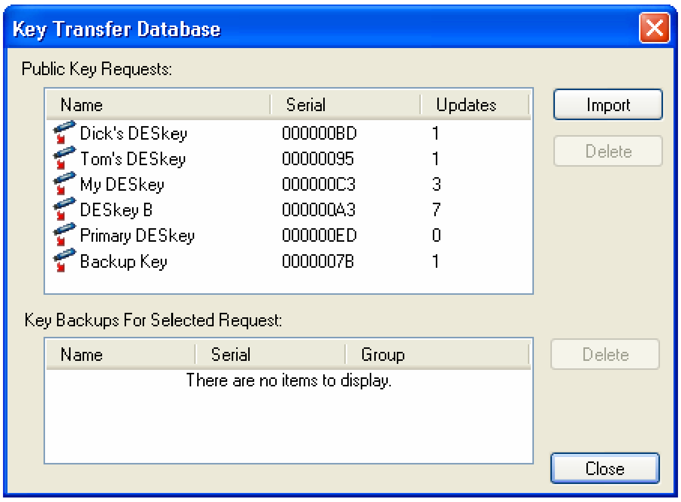
Key My New Key was successfully generated into key slot 3.

Figure 9 - 5

Key Transfer Database

The Key Transfer Database is a database stored on the local machine. It contains public key information for DK5 DESkeys, and also encryption key updates for those DESkeys. Encryption key updates are encryption keys that have been previously extracted with the specified DESkey as the intended destination. The Key Transfer Database is not used when working with a Key-File.

Access to the Key Transfer Database is achieved via the Key Transfer Database applet. This is launched by right clicking the DESlock$^+$ icon in the system tray and selecting **Key Transfer Database**.



Key Transfer Database

Public Key Requests:

Name	Serial	Updates
Dick's DESkey	000000BD	1
Tom's DESkey	00000095	1
My DESkey	000000C3	3
DESkey B	000000A3	7
Primary DESkey	000000ED	0
Backup Key	0000007B	1

Key Backups For Selected Request:

Name	Serial	Group

There are no items to display.

Figure 10 - 1

When encryption keys are backed up, or transferred to another DESkey, the first step is always to extract the encryption key. The encryption key cannot be extracted directly; instead one must specify the DESkey to which the encryption key is destined so it may be securely extracted and protected.

Each DESkey contains a public/private RSA key pair. The public key of a DESkey must be known in order to extract the encryption key. This encryption key is protected with this public key so that it can only be understood by the DESkey with the corresponding (paired) private key. No other DESkey would be able to use the encryption key.

Extracted encryption keys are stored in the key transfer database, encrypted with the recipient's public key. From here they can be deleted if required. To do this, select a DESkey from the "Public Key Requests" list and select the encryption key update from the "Key Backups For Selected

Request" list. Then click the "Delete" button associated with this list.

To delete the public key request for a specified DESkey click the "Delete" button associated with the "Public Key Requests" list. This in turn will delete all encryption key updates associated with that public key.

To add a Public Key Request, click the "Import" button. This will read the public key from an existing DESkey Request (DLR) file which can be created using the Key Transfer Wizard (see page 69).

Key Transfer Wizard

The Key Transfer Wizard has three steps designed to allow encryption keys to be transferred to and from a DK5 DESkey. Key-Files do not support key transfer so the Key Transfer Wizard cannot be used with a Key-File.

Whenever an encryption key is required to decrypt data, but is not present within the active DESkey, it must be requested using this wizard.

The three steps involved in key transfer are:

- Key Request
- Key Issue
- Key Update

The Request and Update steps are performed by the user requesting the key. The Issue step is performed by the user issuing the key.

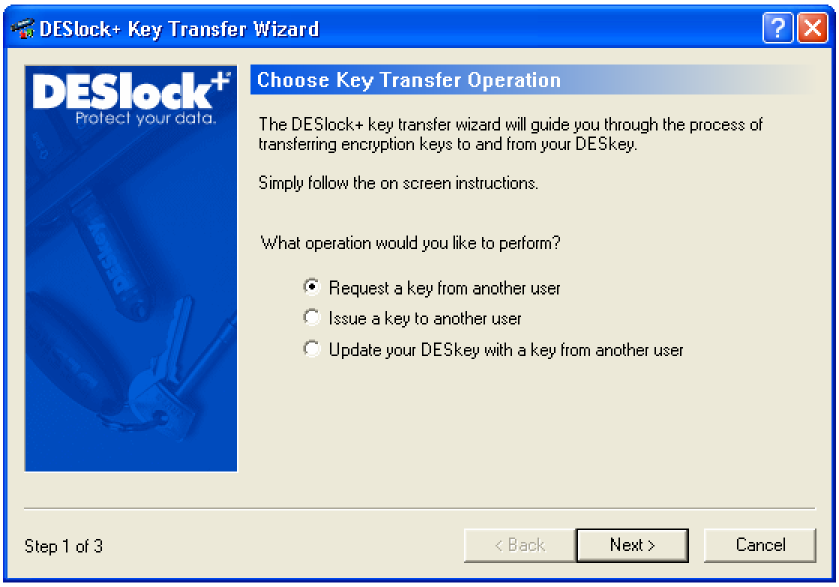
Files used in the key transfer process will have one of the following two icons.

Icon	Meaning
DESkey	A DESkey Request file (file extension .DLR).
DESkey	A DESkey Update file (file extension .DLU).

As files created in the backup process are equivalent to DESkey Update files, the Key Transfer Wizard can also be used to add encryption key backups to a DESkey. The creation of backup files is described on page 60.

Transferring Encryption Keys

When the Wizard is launched normally, the option screen (Figure 11 - 1) is shown.



DESlock+ Key Transfer Wizard

Choose Key Transfer Operation

The DESlock+ key transfer wizard will guide you through the process of transferring encryption keys to and from your DESkey.

Simply follow the on screen instructions.

What operation would you like to perform?

- ● Request a key from another user
- ○ Issue a key to another user
- ○ Update your DESkey with a key from another user

Step 1 of 3

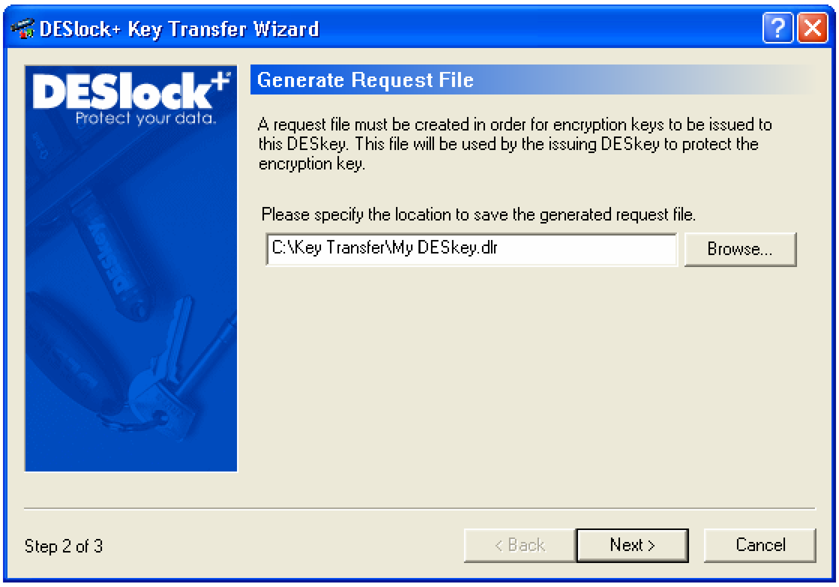
Figure 11 - 1

If the Wizard is launched by the Outlook plug-in, this screen is not shown as the desired action is already known. Similarly, if double clicking on a DLU or DLR file the Wizard will be launched with the appropriate option selected.

Request a key from another user

The request option of the Key Transfer Wizard will create a request file. This file is necessary to issue an encryption key.

Either 'browse' for or manually enter the location and filename to store the request. Click **Next**.



Generate Request File

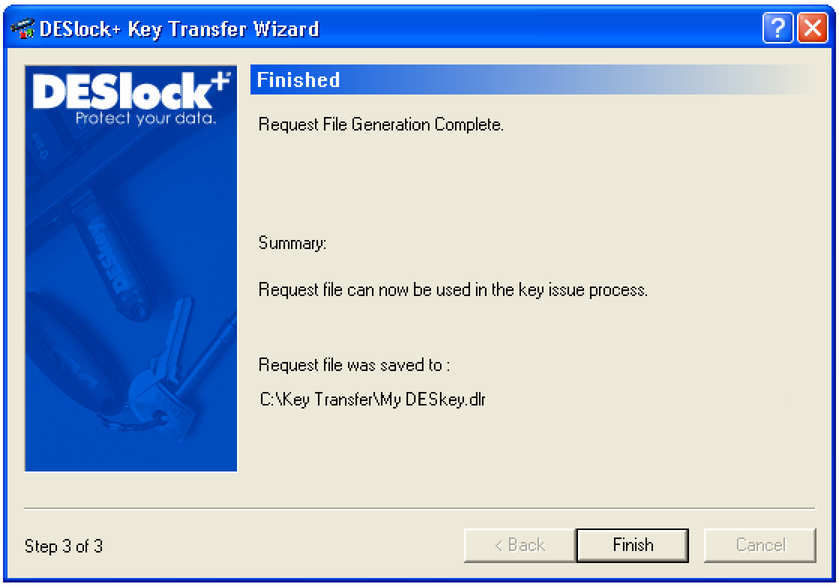
A request file must be created in order for encryption keys to be issued to this DESkey. This file will be used by the issuing DESkey to protect the encryption key.

Please specify the location to save the generated request file.

C:\Key Transfer\My DESkey.dlr

Figure 11 - 2

The request is complete and the request file has been saved to the location specified. This file must now be sent to the issuing DESkey, for example by email.



Finished

Request File Generation Complete.

Summary:

Request file can now be used in the key issue process.

Request file was saved to :

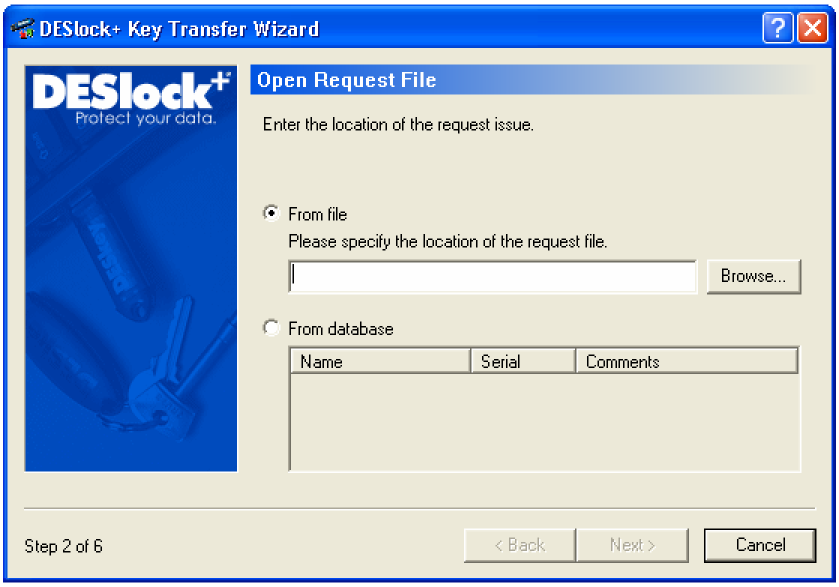
C:\Key Transfer\My DESkey.dlr

Figure 11 - 3

Issue a key to another user

The issue option of the Key Transfer Wizard will extract an Encryption Key and protect it with the requesting DESkeys Public Key. A copy of the Public Key must be available either from details stored in the Key Transfer Database or by using a request file.

Either **Browse** for or manually enter the path and filename of the request file, created by the requesting DESkey. Or alternatively, if it is listed select the DESkey from the Key Transfer Database. Click **Next**.



DESlock+ Key Transfer Wizard

Open Request File

Enter the location of the request issue.

● From file

Please specify the location of the request file.

Name	Serial	Comments

○ From database

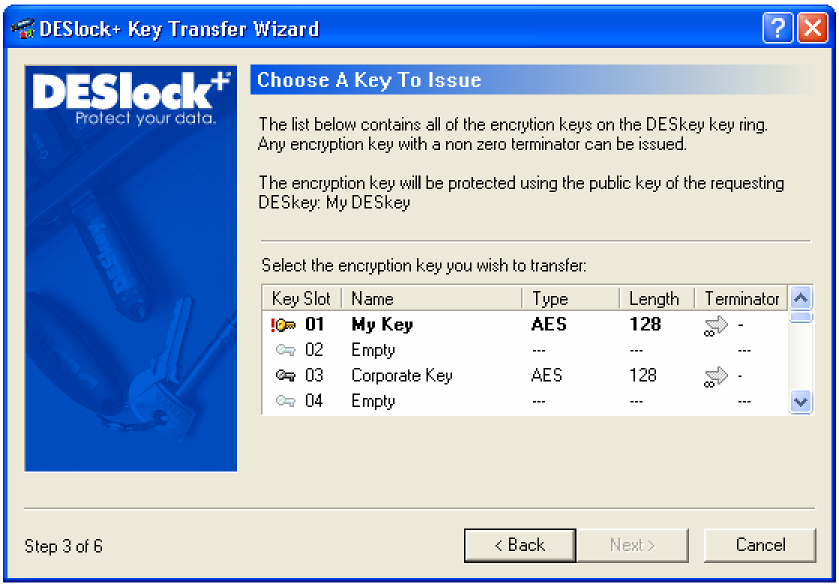
Step 2 of 6

Figure 11 - 4

Details of a DESkey will be stored in the Key Transfer Database if the requesting DESkey was setup using the DESkey Setup Wizard on this machine or the public key was chosen to be added during a previous key transfer operation.

If a request file is used and the key details of the public key are not already stored in the local Key Transfer Database, the user will be given the option of adding the public key here.

Select the encryption key you wish to issue. Any of the keys can be issued provided the Terminator Code is non zero. When the correct key has been selected, click **Next**.



DESlock+ Key Transfer Wizard

Choose A Key To Issue

The list below contains all of the encrytion keys on the DESkey key ring. Any encryption key with a non zero terminator can be issued.

The encryption key will be protected using the public key of the requesting DESkey: My DESkey

Select the encryption key you wish to transfer:

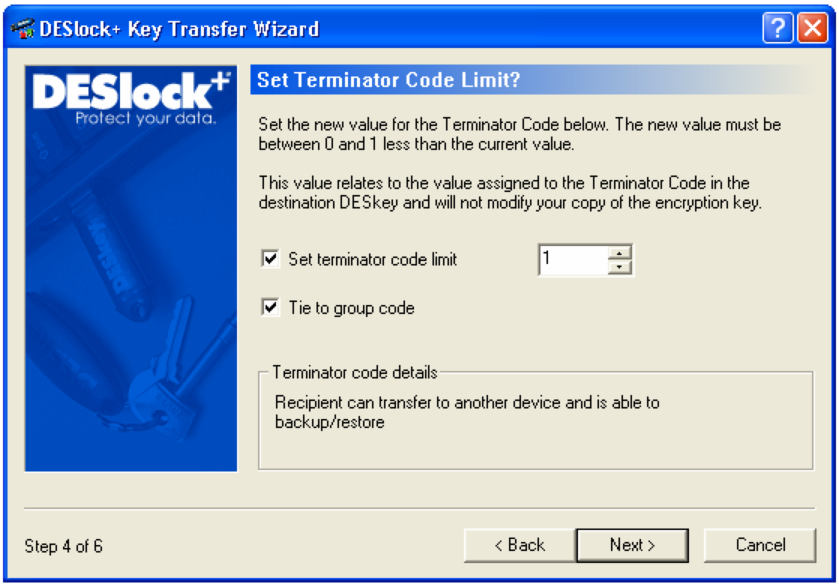
Key Slot	Name	Type	Length	Terminator
01	**My Key**	**AES**	**128**	-
02	Empty	---	---	---
03	Corporate Key	AES	128	-
04	Empty	---	---	---

Step 3 of 6

Figure 11 - 5

Set the new value for the Terminator Code. The new value must be less than the Terminator Code of the encryption key in the issuing DESkey. For example, if the key being issued has a Terminator Code of 5 then the new value must be between 0 and 4 (inclusive). If a value is not explicitly set the default is zero. This value relates to the value assigned to the Terminator Code in the requesting DESkey and will not modify the original copy in the issuing DESkey.

If 'Tie to group code' is selected, this restricts further transfer as the key must stay within the group. The option is only available if the current DESkey is a member of a group.



DESlock+ Key Transfer Wizard

Set Terminator Code Limit?

Set the new value for the Terminator Code below. The new value must be between 0 and 1 less than the current value.

This value relates to the value assigned to the Terminator Code in the destination DESkey and will not modify your copy of the encryption key.

☑ Set terminator code limit 1

☑ Tie to group code

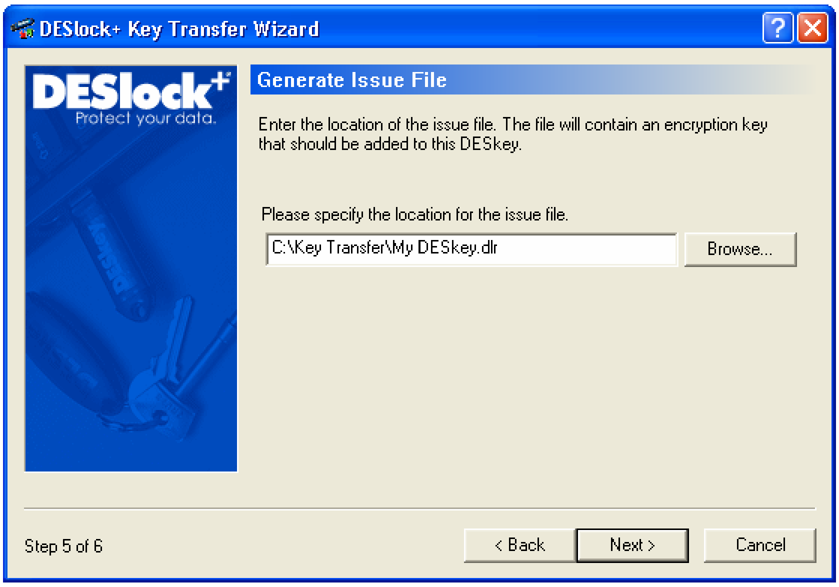
Terminator code details

Recipient can transfer to another device and is able to backup/restore

Step 4 of 6

Figure 11 - 6

Either 'browse' for or manually enter the location and filename for the update file. This file will contain the selected encryption key, protected by the public key of the requesting DESkey so that the key can only be added to the requesting DESkey. This file will need to be used by the requesting DESkey during the update procedure.



Generate Issue File

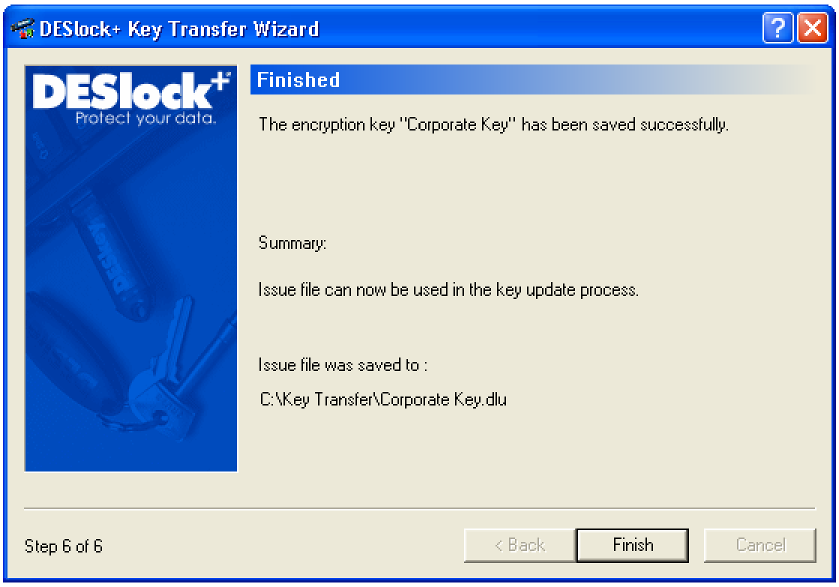
Enter the location of the issue file. The file will contain an encryption key that should be added to this DESkey.

Please specify the location for the issue file.

C:\Key Transfer\My DESkey.dlr

Figure 11 - 7

The Issue is complete and the update file has been saved to the location specified. This file must now be sent to the requesting DESkey.



Finished

The encryption key "Corporate Key" has been saved successfully.

Summary:

Issue file can now be used in the key update process.

Issue file was saved to :

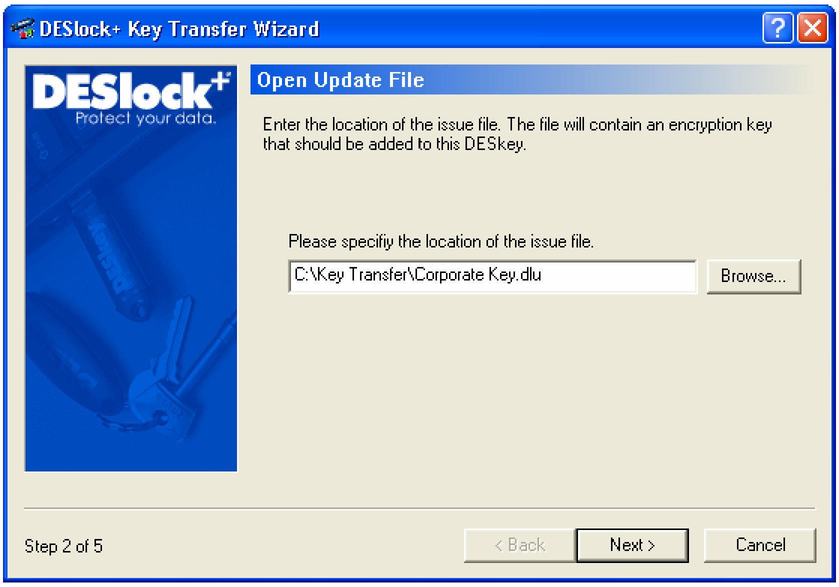
C:\Key Transfer\Corporate Key.dlu

Figure 11 - 8

Update your DESkey with a key from another user

The update option of the Key Transfer Wizard will update your DESkey with an encryption key from another DESkey. This includes encryption keys sent by other users or encryption keys that have been backed up to a file.

Either **Browse** for or manually enter the path and filename of the update file. Click **Next**.



Open Update File

Enter the location of the issue file. The file will contain an encryption key that should be added to this DESkey.

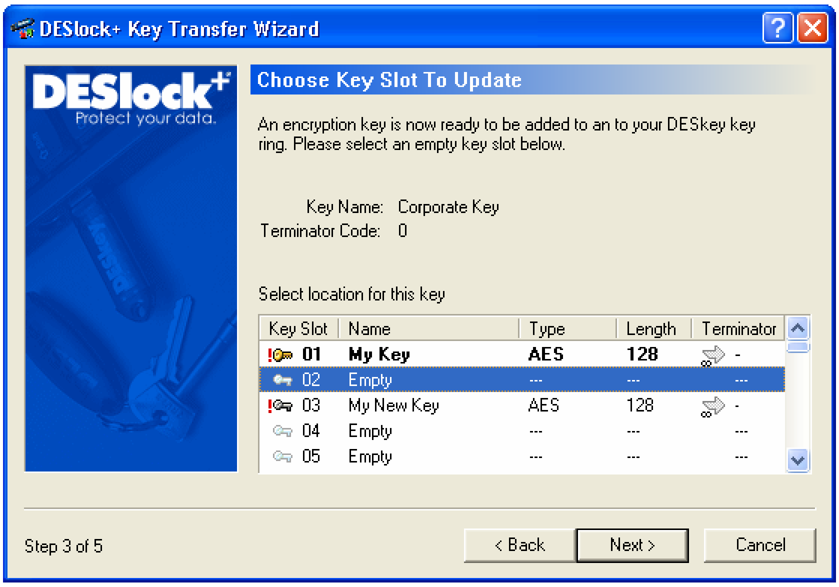
Please specifiy the location of the issue file.

C:\Key Transfer\Corporate Key.dlu

Step 2 of 5

Figure 11 - 9

Once the file has been opened, the location in the key storage space of the DESkey must be specified. The name of the encryption key and the Terminator Code will be displayed. Once a suitable location has been specified click **Next**.



Choose Key Slot To Update

An encryption key is now ready to be added to an to your DESkey key ring. Please select an empty key slot below.

Key Name: Corporate Key
Terminator Code: 0

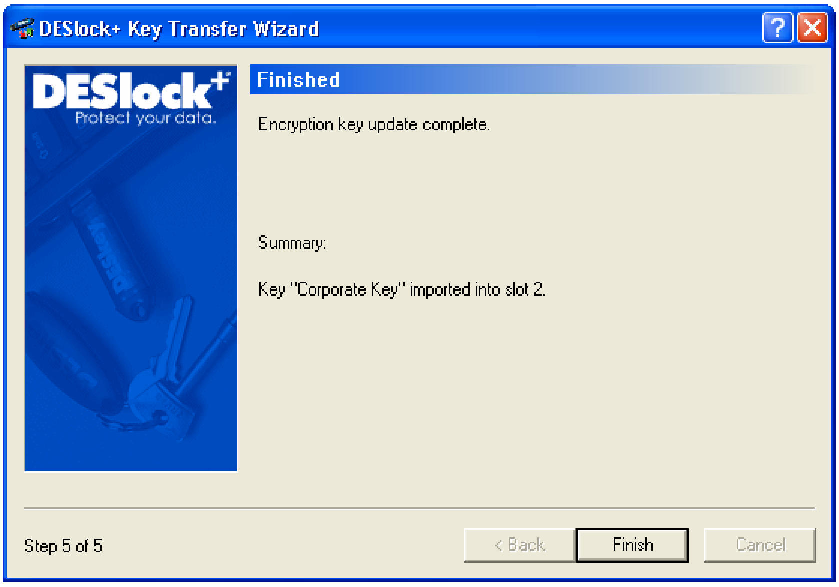
Select location for this key

Key Slot	Name	Type	Length	Terminator
! 01	**My Key**	**AES**	**128**	-
02	Empty	---	---	---
! 03	My New Key	AES	128	-
04	Empty	---	---	---
05	Empty	---	---	---

Step 3 of 5

Figure 11 - 10

The update is complete and this DESkey now contains the new encryption key. Files can now be encrypted or decrypted using this key.



Encryption key update complete.

Summary:

Key "Corporate Key" imported into slot 2.

Figure 11 - 11

Encrypting with DESlock$^+$

There are several ways to encrypt data using DESlock$^+$. Either an entire folder can be encrypted, allowing transparent and automatic encryption and decryption of the files. Individual files can be encrypted or decrypted manually when required. It is also possible to manually encrypt and decrypt text data in programs without needing to encrypt the entire file.

Folder Encryption

The following guide demonstrates encryption of a folder using file system encryption. In this example the folder being encrypted is named 'My Encrypted Documents' and is located on the desktop.

Figure 12 - 1

Right click on the folder from Windows Explorer and choose **Encrypt with DESlock+…** from the context menu. This will launch the Folder Encryption Wizard which will guide you through the encryption process (Figure 12 - 3).

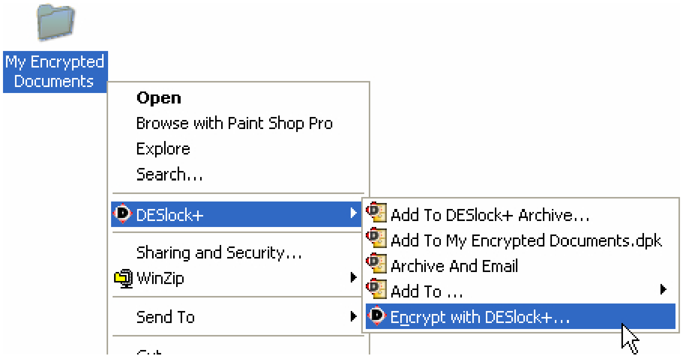
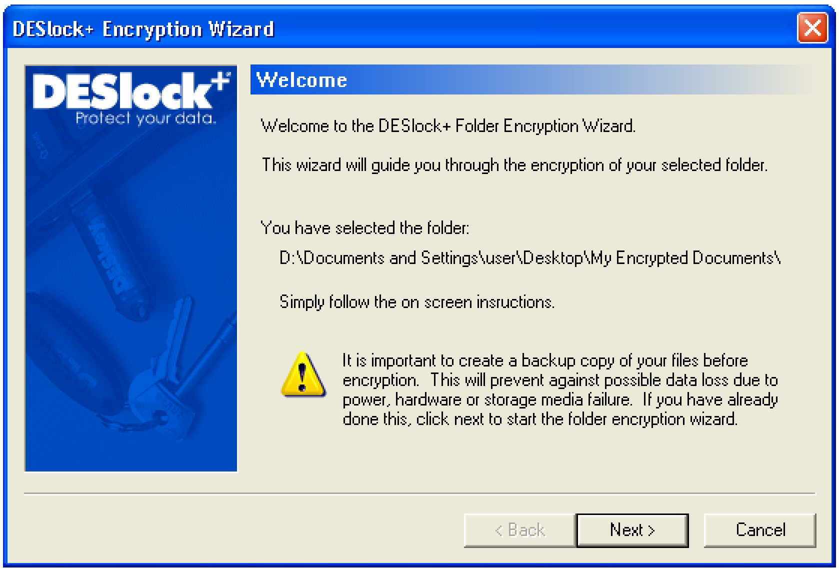


Figure 12 - 2

Please note that not every folder can be encrypted using DESlock$^+$. If DESlock$^+$ determines that a particular folder cannot be encrypted, perhaps because it is a key system folder, then the option to encrypt will not appear. This is to prevent the machine becoming inoperable because folders required by Windows at boot time are unavailable.

DESlock$^+$ may also warn the user that a folder may be unsuitable for encryption if it determines that there is a *chance the machine may be inoperable if the folder was encrypted.*



Welcome

Welcome to the DESlock+ Folder Encryption Wizard.

This wizard will guide you through the encryption of your selected folder.

You have selected the folder:

D:\Documents and Settings\user\Desktop\My Encrypted Documents\

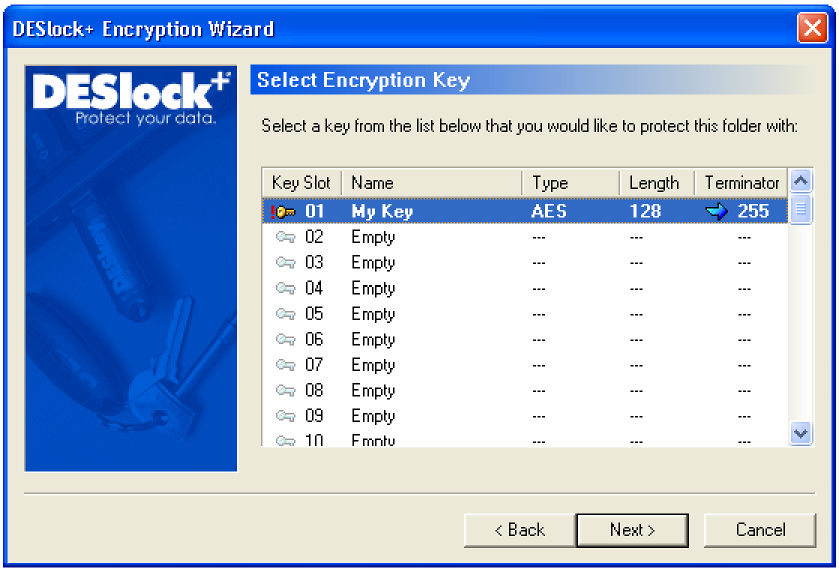
Simply follow the on screen insructions.

It is important to create a backup copy of your files before encryption. This will prevent against possible data loss due to power, hardware or storage media failure. If you have already done this, click next to start the folder encryption wizard.

Figure 12 - 3

You must choose an encryption key to use for the encryption of the folder. Any key listed in the DK5 DESkey key space or the Key-File can be used to encrypt the folder. A password cannot be used to encrypt a folder.

If the only copy of an encryption key is lost there is no way to recover data encrypted using that key. Important keys should be backed up to avoid loss of data.



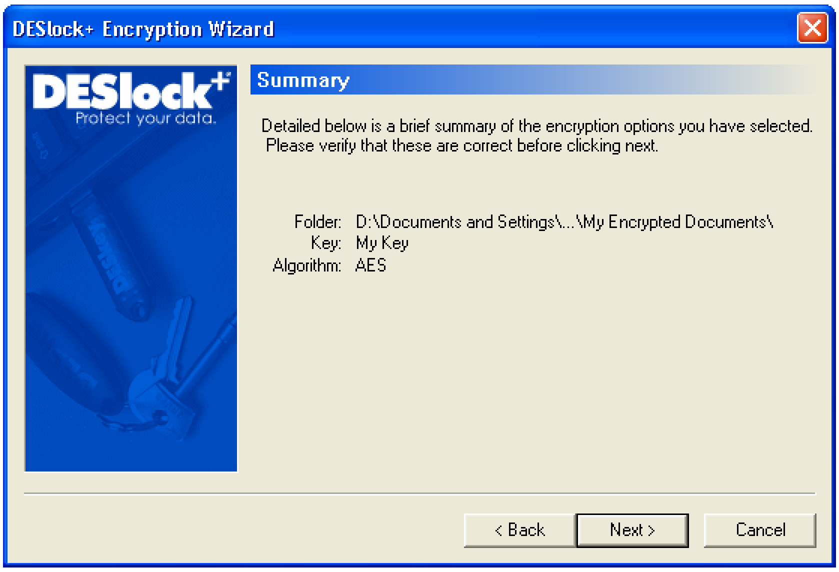
Select Encryption Key

Select a key from the list below that you would like to protect this folder with:

Key Slot	Name	Type	Length	Terminator
01	My Key	AES	128	255
02	Empty	---	---	---
03	Empty	---	---	---
04	Empty	---	---	---
05	Empty	---	---	---
06	Empty	---	---	---
07	Empty	---	---	---
08	Empty	---	---	---
09	Empty	---	---	---
10	Empty	---	---	---

Figure 12 - 4

Before the encryption begins, a summary screen will be shown with the name of the folder being encrypted, the name of the key being used and the algorithm type. If this is satisfactory, click **Next** to begin the encryption process.

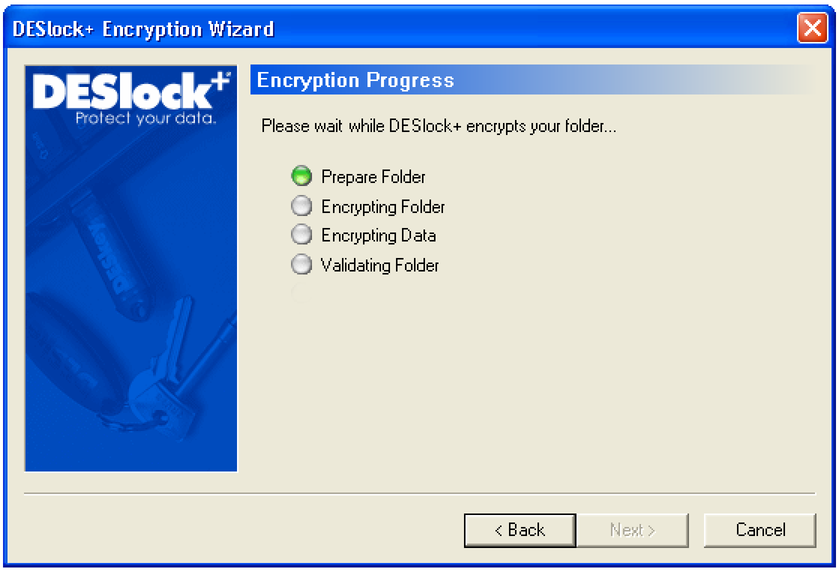


Detailed below is a brief summary of the encryption options you have selected. Please verify that these are correct before clicking next.

Folder: D:\Documents and Settings\...\My Encrypted Documents\
Key: My Key
Algorithm: AES

Figure 12 - 5

When ready to encrypt, click **Start**. As the encryption progresses the icons will turn from their initial state to green. This process may take some time if there are a large number of files in the folder. When complete the folder and all files within, including those within sub folders, will have been encrypted using the specified key.

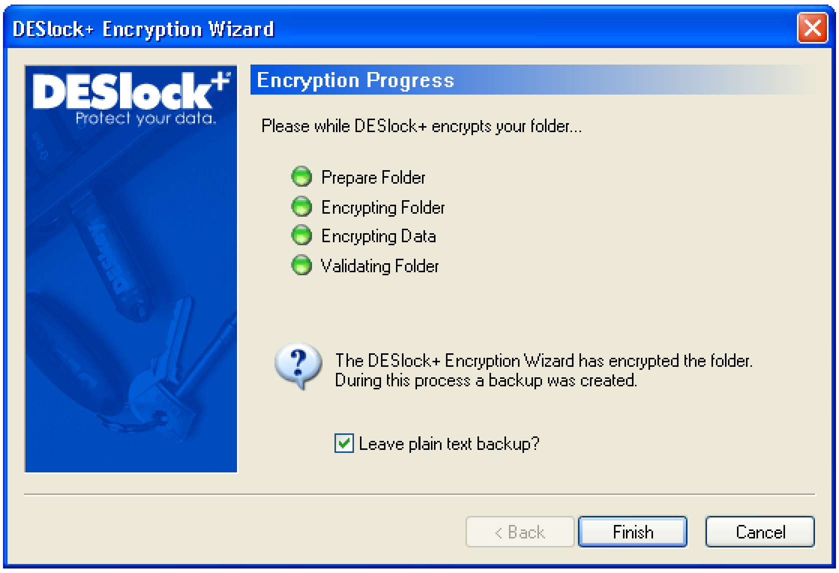


Please wait while DESlock+ encrypts your folder...

● Prepare Folder
○ Encrypting Folder
○ Encrypting Data
○ Validating Folder

Figure 12 - 6

If all tasks were successful, the folder will now be encrypted.



Please while DESlock+ encrypts your folder...

- Prepare Folder
- Encrypting Folder
- Encrypting Data
- Validating Folder

The DESlock+ Encryption Wizard has encrypted the folder.
During this process a backup was created.

☑ Leave plain text backup?

Figure 12 - 7

Once the folder has been encrypted, any files copied to, moved to or created in the folder, including sub folders, will be automatically protected.

Note that an encrypted folder will have the following icon

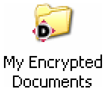


Figure 12 - 8

It is important to note that during the encryption process a copy of the original data will have been made and saved in a folder of the same name but with the suffix "(DLP Backup)". If you do not want this backup to be saved you may uncheck the box on the final wizard screen.

Decryption

If a folder has already been encrypted, right click on the folder from Windows Explorer and choose 'Decrypt with DESlock+…' from the context menu if you want to decrypt the folder and all of its contents.

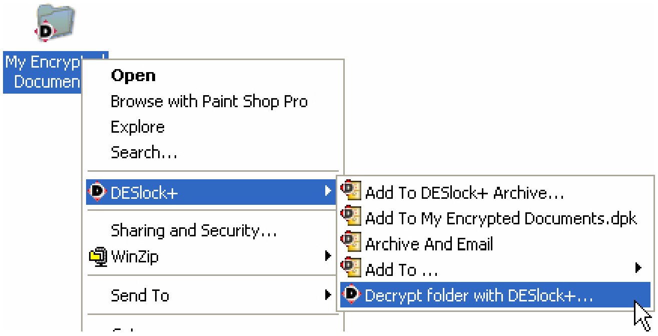

My Encrypted Documents
Open
Browse with Paint Shop Pro
Explore
Search...
DESlock+
Sharing and Security...
WinZip
Send To
Add To DESlock+ Archive...
Add To My Encrypted Documents.dpk
Archive And Email
Add To ...
Decrypt folder with DESlock+...

Figure 12 - 9

Encrypting Network Shares

It is not possible to encrypt a folder on a network drive. For network drives, you should use a DESlock$^+$ Mountable File. The file can reside on a network location and can be mounted from there when necessary. DESlock$^+$ Mountable Files are described in more details on page 89.

Individual File Encryption

DESlock+ can also integrate with the Windows shell to allow encryption and decryption of individual files. This allows files to be encrypted enabling them to be transferred securely, remaining in encrypted format. Please note that this is not the same as folder encryption (described earlier on page 77) as encryption and decryption is not automatic, although the same encryption keys and algorithms can be used in both cases.

The shell integration allows files to be encrypted or decrypted after 'right-clicking' on them (Figure 12 - 10).

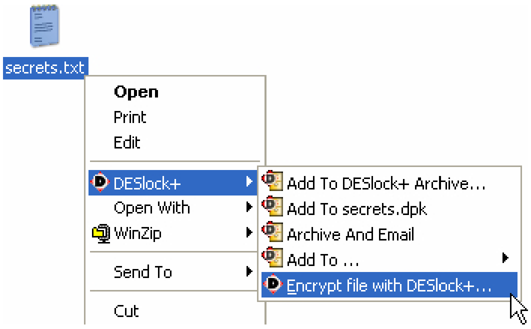


Figure 12 - 10

The available menu options are:

Encrypt files with DESlock+

If one or more files are selected, and they are all non encrypted, this option will encrypt them all. The user must choose either an encryption key to use for encryption, or must specify a password. If encrypting multiple files at the same time, the same encryption key will be used.

After encryption, the original files will remain intact and encrypted copies will be made in the same folder. The encrypted copies will have a DLP extension and the following icon.

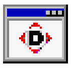


Figure 12 - 11

Decrypt files with DESlock+

If one or more files are selected, and they are all encrypted, this option will decrypt them.

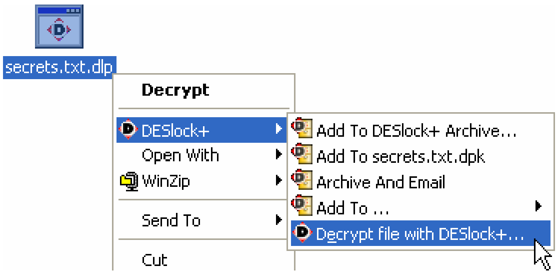


Figure 12 - 12

After decryption, the original files can be deleted or left intact. The desired action can be changed in the DESlock$^+$ Control Panel (described on page 44).

Please note that decryption will only occur if the correct encryption key is present in the currently active DESkey, or the correct password is entered.

Process files with DESlock+

If one or more files are selected, and they are a combination of encrypted and non-encrypted, this option will process them individually following the above rules. That is, if a particular file is non-encrypted it will be encrypted and conversely if it is encrypted it will be decrypted.

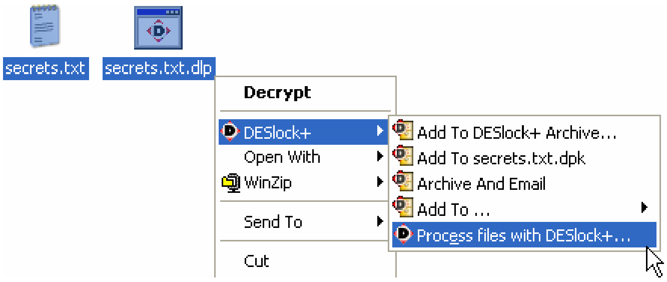


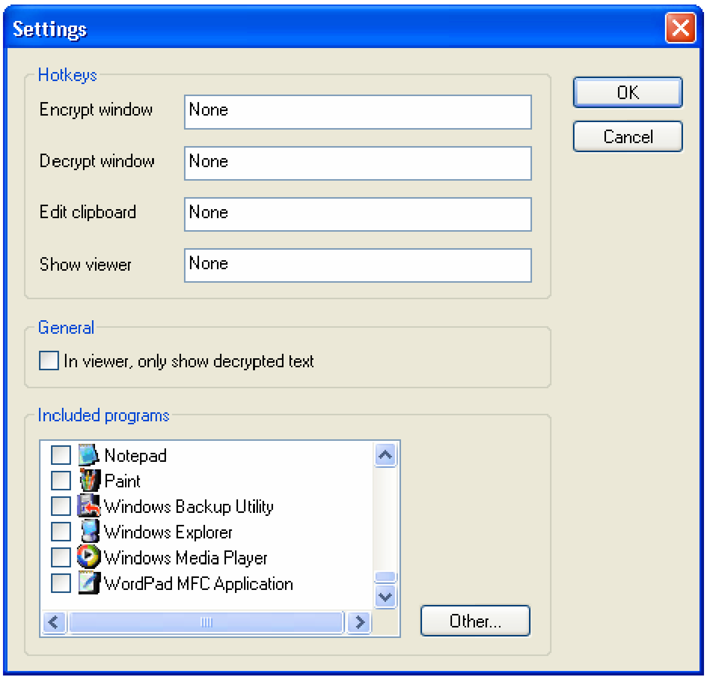
Figure 12 - 13

Individual File Encryption is compatible with the Outlook Plug-in, meaning it can be used to send or receive encrypted message attachments with another user using the Outlook Plug-in.

DESlock$^+$ Tools

DESlock$^+$ Tools is a utility that integrates with most Windows applications to allow encryption and decryption of text within a window.

To use DESlock$^+$ Tools in an application you should ensure it is enabled for that application. To do this choose the Tools, Settings menu from the DESlock$^+$ System Tray icon. This will bring up the Settings window, where you can set hotkeys for encryption/decryption with DESlock$^+$ tools, and also set which applications will display DESlock$^+$ Tools options. Check those applications you wish to use DESlock$^+$ tools with. The other button can be used to add applications to the list.



Settings

Hotkeys

Encrypt window: None

Decrypt window: None

Edit clipboard: None

Show viewer: None

General

□ In viewer, only show decrypted text

Included programs

□ Notepad
□ Paint
□ Windows Backup Utility
□ Windows Explorer
□ Windows Media Player
□ WordPad MFC Application

Figure 12 - 14

When a program has been included, the system menu will display a DESlock^{+} menu which enables the encryption or decryption of the current window contents.

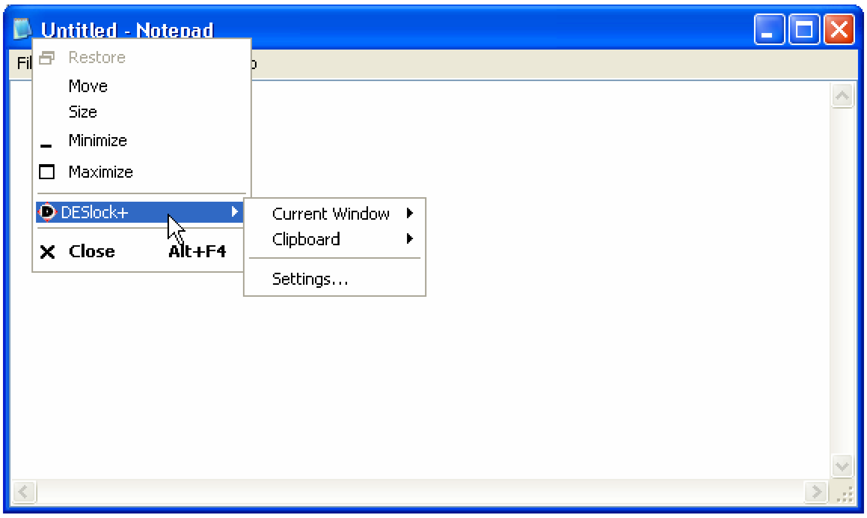


Figure 12 - 15

If an application has not been included, DESlock^{+} Tools can still be used but it must be accessed through the DESlock^{+} System Tray icon.

Any selected text in the current window, or text in the clipboard, can be encrypted or decrypted with DESlock^{+} Tools.

DESlock^{+} Tools is compatible with the Outlook Plug-in, meaning it can be used to send or receive encrypted messages with another user using the Outlook Plug-in.

Offline encrypted folders

It is possible to protect a local cached copy of a non-encrypted network folder, in a similar manner to the standard Windows offline folder support. This is useful where network resources are required to be taken off site and the offline copy must remain secure.

To make an encrypted local copy available, right click on the network folder and choose **Make local encrypted copy** from the **DESlock+** menu item.

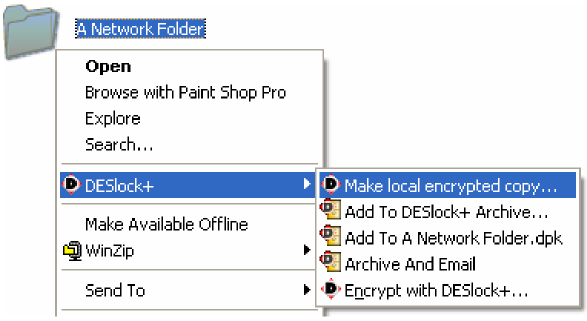
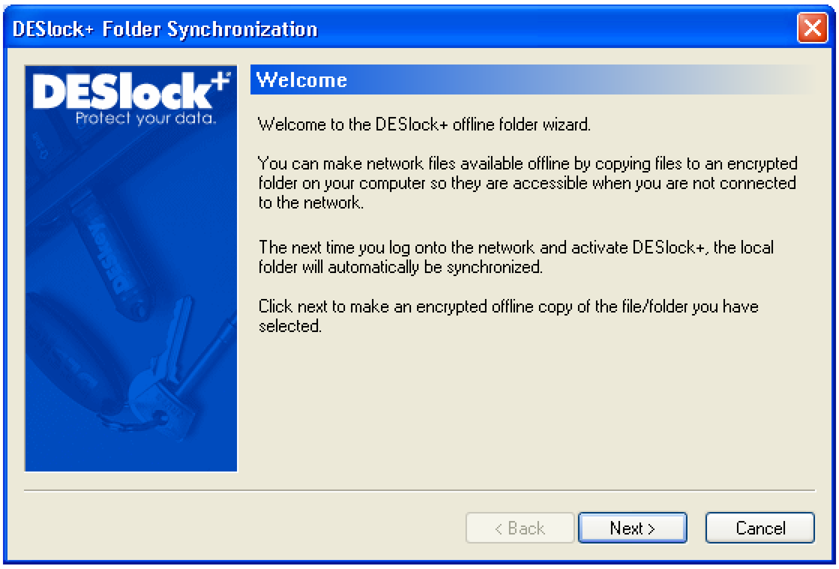


Figure 12 - 16

Next, the folder synchronisation wizard will guide you through the synchronisation process. The initial time this is run, the user is prompted to choose an encryption key, to be used to encrypt the data locally, and also specify the local folder to store the synchronised data in.



Welcome to the DESlock+ offline folder wizard.

You can make network files available offline by copying files to an encrypted folder on your computer so they are accessible when you are not connected to the network.

The next time you log onto the network and activate DESlock+, the local folder will automatically be synchronized.

Click next to make an encrypted offline copy of the file/folder you have selected.

Figure 12 - 17

When the folder has been synchronised the icon will change to reflect the status.

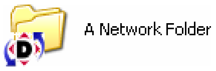


Figure 12 - 18

The synchronised folders are accessible via the 'DESlock+ Offline Folders' icon in My Computer or by browsing directly to the synchronised folder store, specified during the initial synchronisation phase.

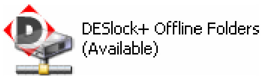


Figure 12 - 19

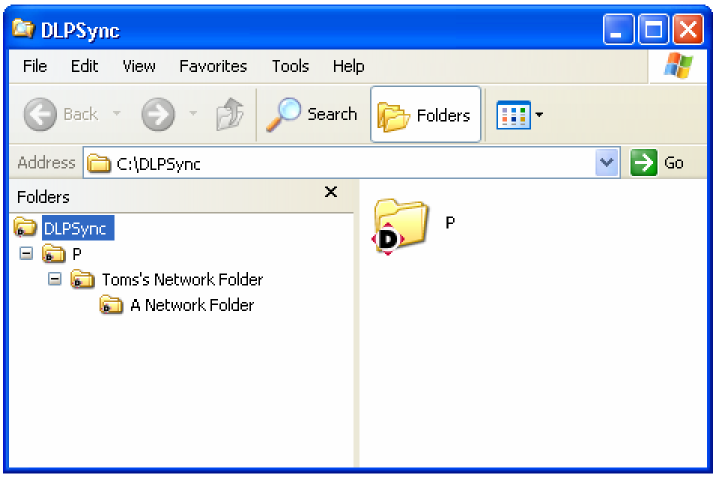


Figure 12 - 20

The folder structure used is based on the path of the network folder. In this case the path was:

```
p:\tom's network folder\a network folder
```

This page has been intentionally left blank

DESlock$^+$ Mount Manager

The DESlock$^+$ Mount Manger is designed to allow a special type of DESlock$^+$ encrypted file to be mounted by Windows and accessed as a normal volume or drive. Such an encrypted file is designed to be placed on any existing media, be it an existing local drive, a network drive, removable media. It can also be used in any location where standard DESlock$^+$ folder encryption is not desired or is not suitable.

The DESlock$^+$ Mount Manager program is accessible via the DESlock$^+$ System Menu. This feature is only available on Windows 2000 or later.

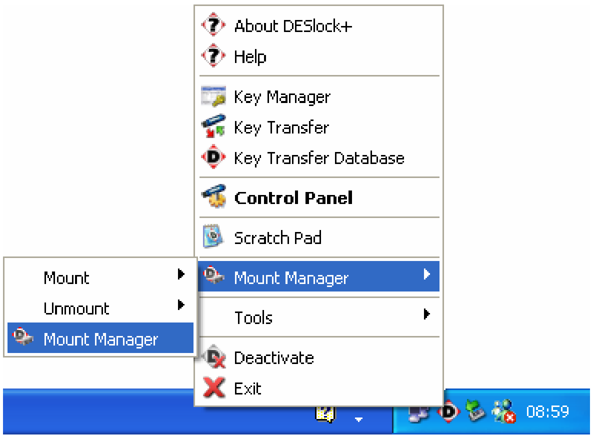


Figure 13 - 1

Creating a Mountable File

To create a mountable file, run the Mount Manager application. Click the **Create** button to create a new mountable file, or the Open button to open an existing mountable file.

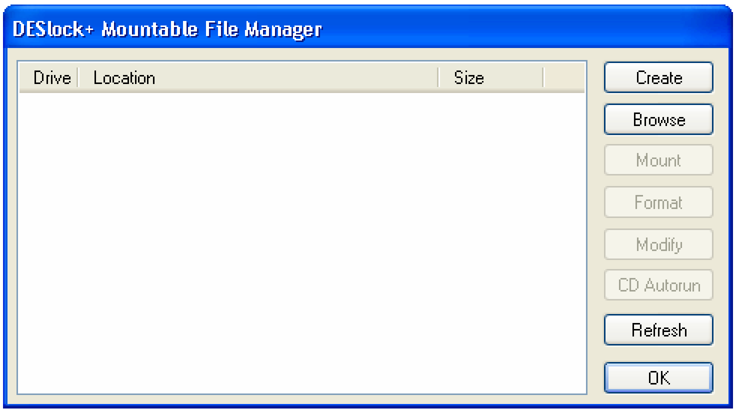
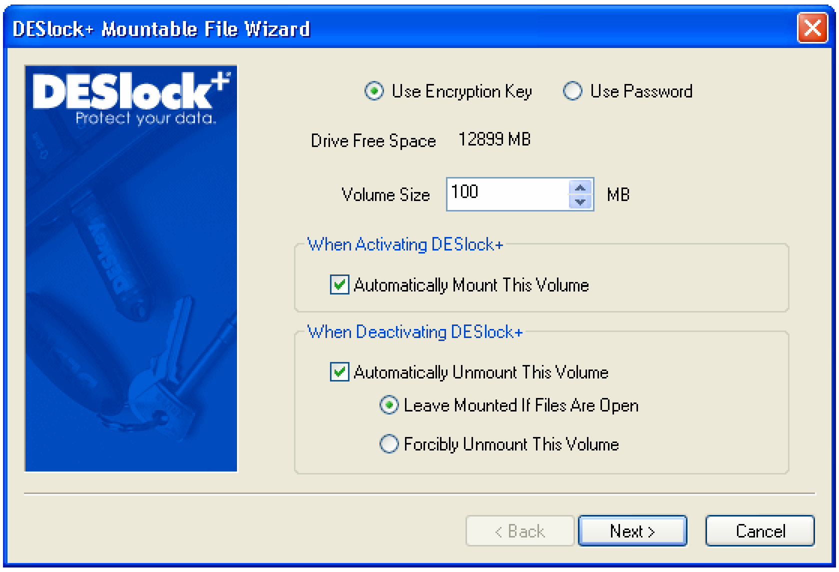


Figure 13 - 2

If creating a new file, first enter a file name and location to store the file. Next, you must enter the attributes of the file (see Figure 13 - 3).

First choose to encrypt the Mountable File with an encryption key or a password. The **Volume Size** setting specifies the size of the drive that this file will provide. By default, this will be 10% of the available space on the hard disk the file is located; The minimum disk size is 10MB. This value cannot be modified once the file has been created so the drive provided will be of fixed size.


DESlock+ Mountable File Wizard

● Use Encryption Key ○ Use Password

Drive Free Space 12899 MB

Volume Size 100 MB

When Activating DESlock+

☑ Automatically Mount This Volume

When Deactivating DESlock+

☑ Automatically Unmount This Volume

● Leave Mounted If Files Are Open

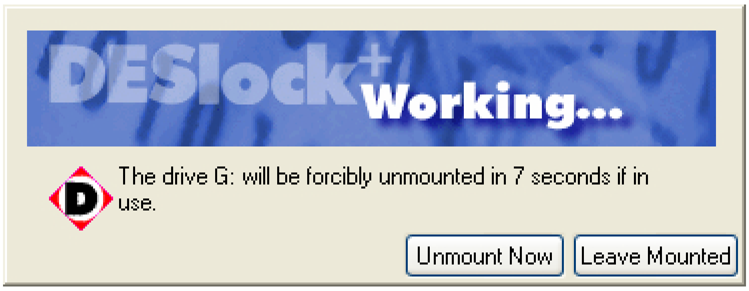
○ Forcibly Unmount This Volume

Figure 13 - 3

The **Automatically Mount This Volume** option directs DESlock$^+$ to attempt to mount the drive when DESlock$^+$ is activated and the correct encryption key is present. This is not applicable if the volume is protected with a password and the volume must be mounted manually.

The **Automatically Unmount This Volume** option directs DESlock$^+$ to attempt to dismount the volume when DESlock$^+$ is deactivated. Please note that this option is only available on Windows XP or later as Windows 2000 does not support dismounting of these mountable files.

By choosing the relevant option, the dismount can be deferred if DESlock$^+$ detects that any of the files stored on the drive are still open or it can be forcibly dismount the drive even if files are still open. A warning (Figure 13 - 4) will be displayed immediately prior to the dismount operation allowing the user time to save their work onto the drive.

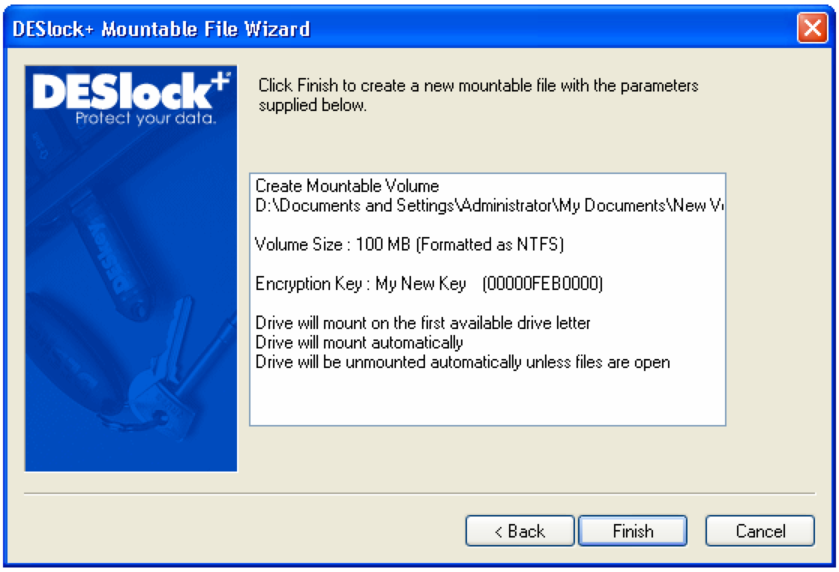


The drive G: will be forcibly unmounted in 7 seconds if in use.

Figure 13 - 4

If files are open, the dismount can be cancelled by clicking the **Leave Mounted** button. This button will only have an affect if files are open. If no files are open on the encrypted drive, the dismount cannot be cancelled.

Once the drive options have been set, the Wizard will prompt for the encryption key to use to protect the volume or will require the user to enter the mount password, depending on the option previously selected. Once a suitable encryption key has been chosen or a password entered, the Wizard will show a summary screen.



Click Finish to create a new mountable file with the parameters supplied below.

Create Mountable Volume
D:\Documents and Settings\Administrator\My Documents\New V

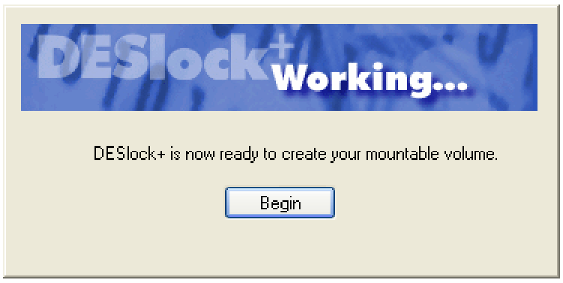
Volume Size : 100 MB (Formatted as NTFS)

Encryption Key : My New Key (00000FEB0000)

Drive will mount on the first available drive letter
Drive will mount automatically
Drive will be unmounted automatically unless files are open

Figure 13 - 5

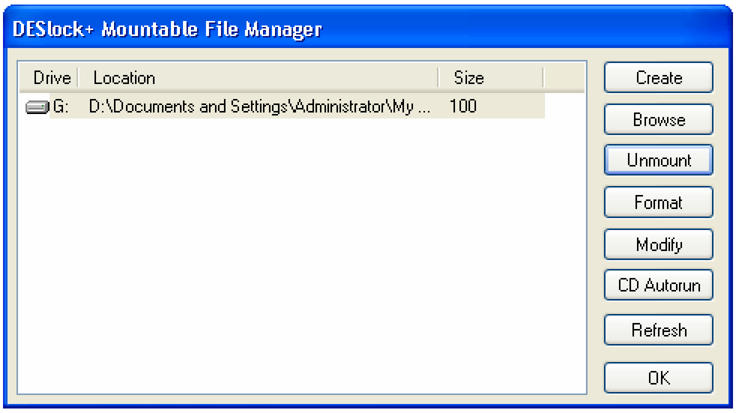
If all details are correct, click **Finish** to create the file. The file will then be formatted as an NTFS volume.



DESlock+ is now ready to create your mountable volume.

Figure 13 - 6

The file will then appear in the Mount Manager and can be mounted. Click the **Mount** button to mount the file, it will be assigned the first available free drive letter.



DESlock+ Mountable File Manager

Drive	Location	Size
G:	D:\Documents and Settings\Administrator\My ...	100

Figure 13 - 7

When the file has been mounted, it will appear as a new drive in 'My Computer' and can be accessed in the same way as any other drive would be.

Figure 13 - 8

The Mount Manager application can also be used to format the drive at any time. Although the drive can be formatted by Windows, we recommend that you always use the Mount Manager to do this.

Once the entry appears in the Mount Manager, the file may be mounted and dismounted in future from the DESlock$^+$ system tray menu.

CD Autorun

The **CD Autorun** button is used to create the autorun files for a CD. This allows a mountable file on a CD to be automatically mounted on insertion of the CD.

To create a CD Autorun for a mountable file, select the image from the list and click the **CD Autorun** button. This will create a folder on the machine with the same name as the currently selected mountable file, and in it place the autorun files.

You should then ensure the mountable file has been dismounted and copy it into this folder along with the autorun.exe and autorun.inf files. You can then burn the contents of this folder onto the root of a CD or DVD.

When the CD or DVD autoruns on a machine with DESlock$^+$, it will automatically attempt to mount the file.

Using Mountable Files

DESlock$^+$ mountable files provide a virtual drive on the PC on which the file has been mounted. The file itself can be stored on any location accessible by the PC, either on a local drive or on a network path.

Shared Access

If the file is stored on a network path, it can be mounted and dismounted as if it were a local file. However, because it is in a shared location, it is possible that another user could also access the file at the same time. If two users attempt to mount the file at the same time, then only one will be successful in mounting the file with read and write access to the drive. Any additional users who then mount the file only be able to access the drive with read access.

Users with read access to the volume will be able to access files within and will see changes made to them, but will not see changes made to the file system, such as new files or folders being added. A user must dismount the drive and remount it to see any changes to the file system.

Windows File and Sharing

DESlock$^+$ cannot be used to directly encrypt a folder that is shared with Windows file sharing, however a folder within a DESlock$^+$ mountable file may be shared. Standard share permissions can be used on the folder meaning multiple users can share write access to the folder. While the share is active, the volume cannot be dismounted however.

Dismounting the volume

The volume cannot be dismounted under Windows 2000. This should be considered especially when attempting to use the mountable file in a shared environment.

Important Notice

Encryption Key Caching

Please be aware that the DESlock$^+$ mountable file works differently than the standard encrypted folders in that the required encryption key is cached for the duration the drive is mounted.

This means that performance of the drive is faster than it would be with a normal encrypted folder.

However, it means that the drive may continue to be available even if DESlock$^+$ is deactivated. The automatic dismount option can be used to attempt to dismount the drive on deactivation of DESlock$^+$.

The encryption key is only required to mount the drive, but once mounted files can be accessed without using DESlock$^+$ again. This means the files are accessible until the drive is dismounted.

Please be aware therefore, that **once mounted unless the drive is dismounted any user can access the drive even if DESlock$^+$ has been deactivated**.

DESlock$^+$ Archive

The DESlock$^+$ Archive is a tool that allows a number of files to be combined in an archive, being stored compressed and encrypted.

The DESlock$^+$ Archive options are available from the DESlock$^+$ context menu, when clicking on a suitable file.

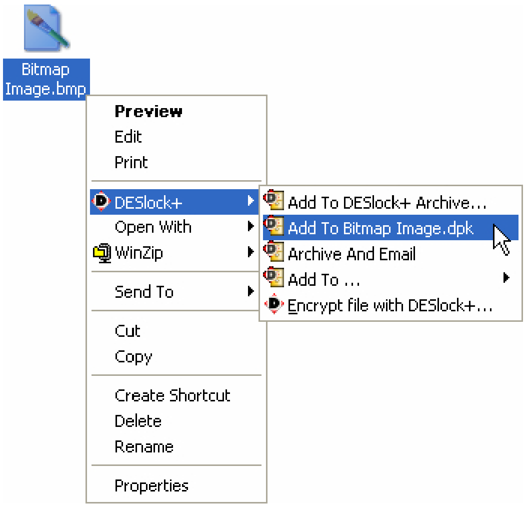
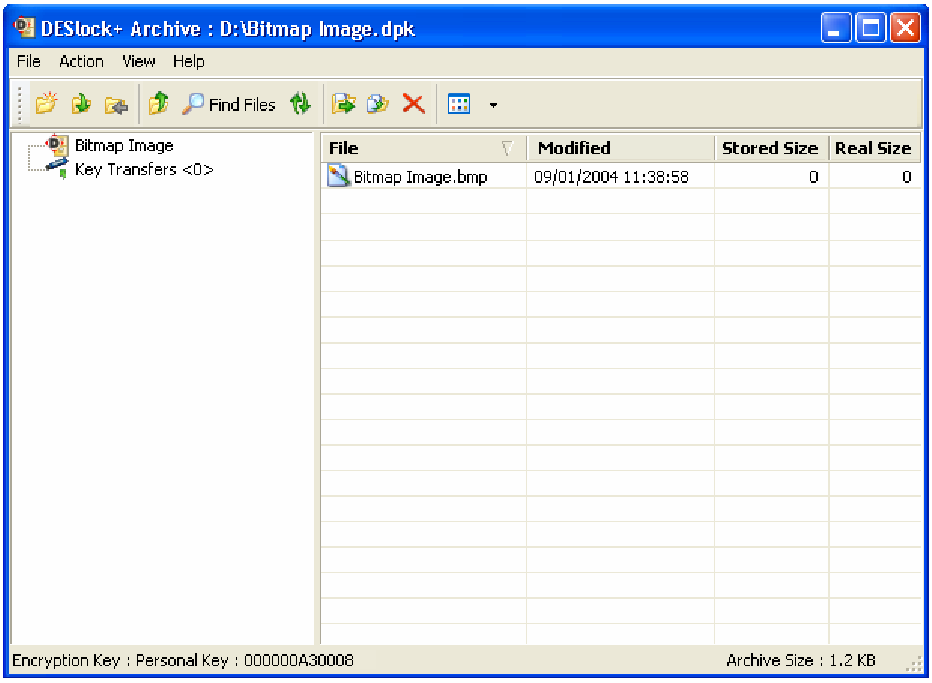


Figure 14 - 1

The available options allow the user to:

- Add the file to an archive of the same name as the file, in the same folder.
- Add the file to a new archive and then prompt to save it.
- Add the file to an archive and then attach it to an email.
- Add the file to a new existing DESlock$^+$ archive in the same folder as the file.

When an archive is created for the first time, an encryption key must be chosen. This encryption key will be used to encrypt all files in the archive.



File	Modified	Stored Size	Real Size
Bitmap Image.bmp	09/01/2004 11:38:58	0	0

Encryption Key : Personal Key : 000000A30008

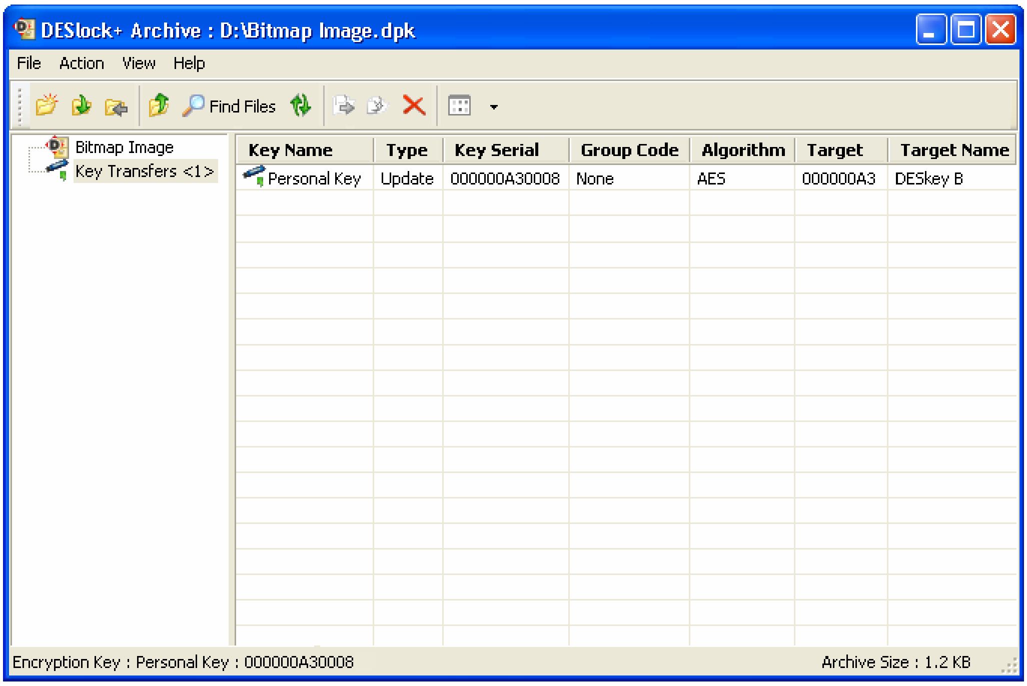
Archive Size : 1.2 KB

Figure 14 - 2

If the archive has been created with an encryption key from a DK5 DESkey that the intended recipient does not have, it is possible to include the encryption key based on a key request from the recipient's key. This request can be generated using the Key Transfer Wizard (see page 69). The key update can then be created and attached using the **Add key update using request file** on the Action menu. Alternatively key updates can be dragged and dropped on the Archive window.

An encryption key from a Key-File cannot be added to a DESlock+ Archive.

If any encryption keys have been included with the archive, these will be available under the key transfer section.

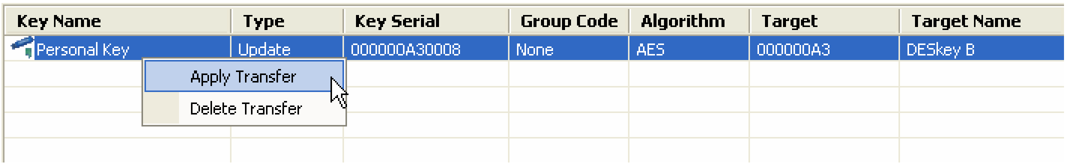


Key Name	Type	Key Serial	Group Code	Algorithm	Target	Target Name
Personal Key	Update	000000A30008	None	AES	000000A3	DESkey B

Encryption Key : Personal Key : 000000A30008 Archive Size : 1.2 KB

Figure 14 - 3

To import the encryption key, right click on the key and choose **Apply Transfer** from the context menu



Key Name	Type	Key Serial	Group Code	Algorithm	Target	Target Name
Personal Key	Update	000000A30008	None	AES	000000A3	DESkey B

Figure 14 - 4

This will then launch the update phase of the key transfer utility. If the encryption key is not available in the currently active DESkey (i.e. it has not been imported), the files in the archive will remain inaccessible.

To extract files from a DESlock+ Archive, one can either drag the files out from the main window into the desired folder, or one may choose to extract the files using the context menu.

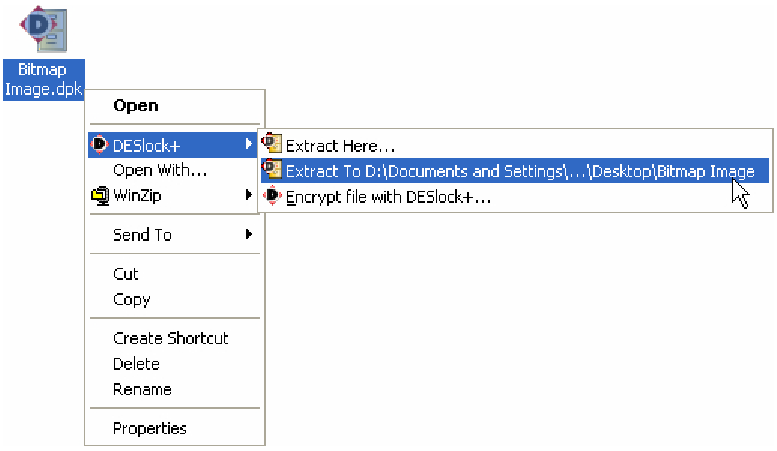


Figure 14 - 5

Outlook Plug-in

The DESlock^{+} Outlook Plug-in is designed to integrate with Microsoft (R) Outlook 98 or later to provide DESlock^{+} encryption of emails and email attachments. The Outlook Plug-in does not integrate with Outlook Express.

If Outlook is not being used, email messages and attachments can still be manually encrypted to retain security. Please refer to the DESlock^{+} Tools (see page 84) and Individual File Encryption (see page 82) documentation.

Outlook Integration

When installed the Outlook Plug-in will add a DESlock^{+} menu to the menu bar and a DESlock^{+} icon (Figure 15 - 1) to the toolbar of the main Outlook window (Figure 15 - 2).

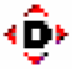


Figure 15 - 1

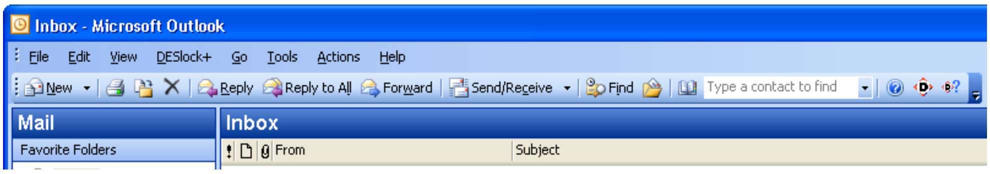
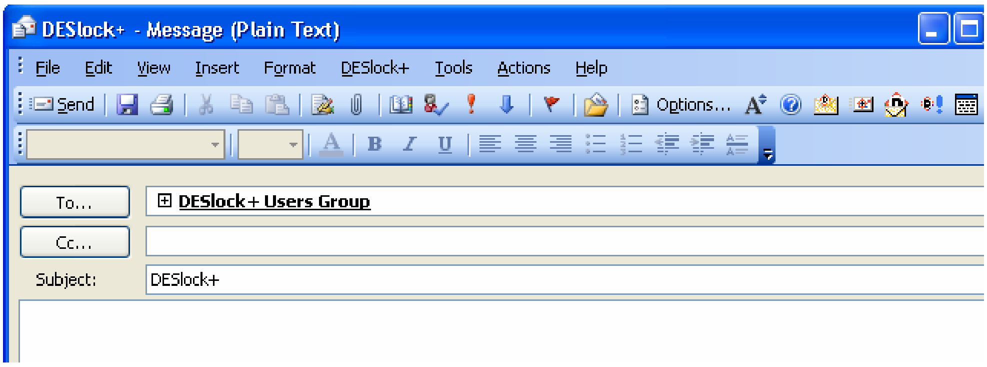

Inbox - Microsoft Outlook
File Edit View DESlock+ Go Tools Actions Help
New Reply Reply to All Forward Send/Receive Find Type a contact to find
Mail
Favorite Folders
Inbox
From
Subject

Figure 15 - 2

In addition to the changes to the main Outlook window, each email message window has additional toolbar icons and DESlock^{+} menu (e.g. shown in Figure 15 - 3).


DESlock+ - Message (Plain Text)
File Edit View Insert Format DESlock+ Tools Actions Help
Send Options...
To...
Cc...

To... DESlock+ Users Group

Subject: DESlock+

Figure 15 - 3

Email Options

Each Outlook email message window may contain the icons listed below which provide additional email options. The options are also available from the DESlock^{+} menu in the message window. The appropriate set of options depends on whether the user is the sender or recipient of an email. Some options may be unavailable depending on the mail format.

Sender Options

Icon	Meaning
	Decrypt for Reply: When replying or forwarding a message, automatic decryption of the quoted message is disabled. Click this button to decrypt the previous message. This is only possible if the originator of the encrypted message has not chosen the Force Viewer option.
	Encrypt and Send: Click this button to encrypt the body of the email, including any attachments, and immediately send the email in one action.
	Encrypt on Send: Click this button to encrypt the email body before sending. The email body will not be encrypted until the email is sent.
	Encrypt Now: Click this button to immediately encrypt the email body. The message can be further edited before being sent. Attachments will not be encrypted immediately but 'Encrypt Attachments' can still be used.
	Force Viewer: Click this button to force the recipient of the email to use the DESlock^{+} Message Viewer (Figure 11 - 4), rather than allow the email to be decrypted in place.

Recipient Options

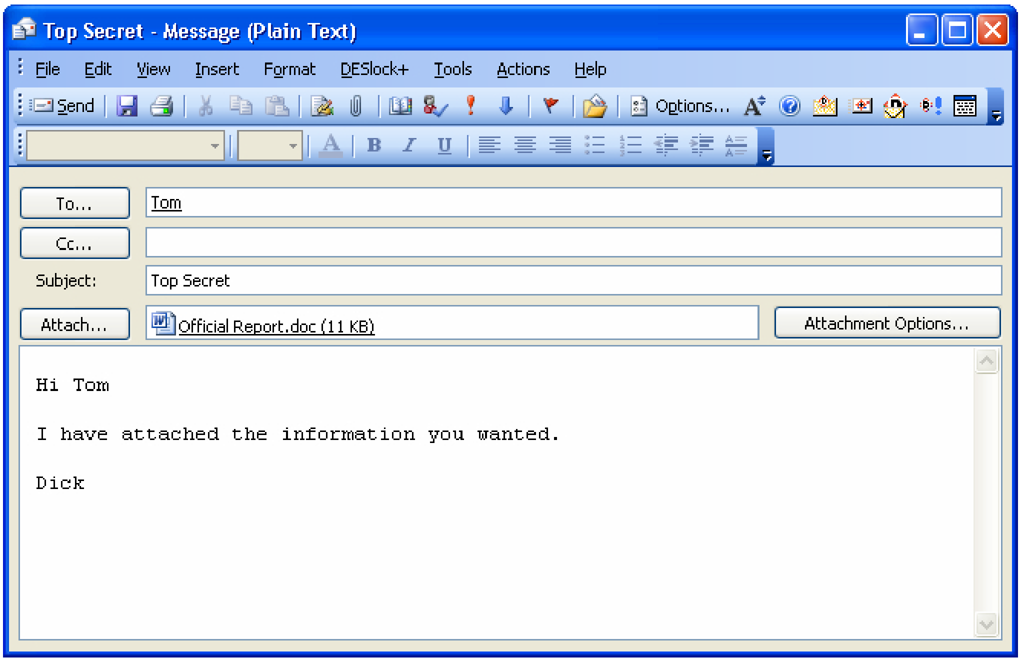
Icon	Meaning
	Decrypt Now: Click this button to decrypt a DESlock^{+} encrypted message.
	Decrypt All Attachments: Click this button to decrypt and save all attachments from the email to a user specified folder. The user must then 'browse' to an existing folder in which to save the files.

	Encrypt This Message: Click this button to encrypt any plain text message. This can include any messages received from a user who is not using DESlock$^+$.

Encrypting a message

When encrypting a message, the user has two options. Either to encrypt the email and send it using either 'Encrypt on Send' or 'Encrypt and Send'. Or the user can encrypt the message and add additional text that can either be encrypted using a different encryption key or can be left in plain view.

In this example we shall choose to encrypt the message and edit it before sending. Below is the original message before clicking the 'Encrypt Now' button.


Top Secret - Message (Plain Text)
File Edit View Insert Format DESlock+ Tools Actions Help
Send
Options...
To...
Cc...
Subject:
Attach...
Attachment Options...

To: Tom

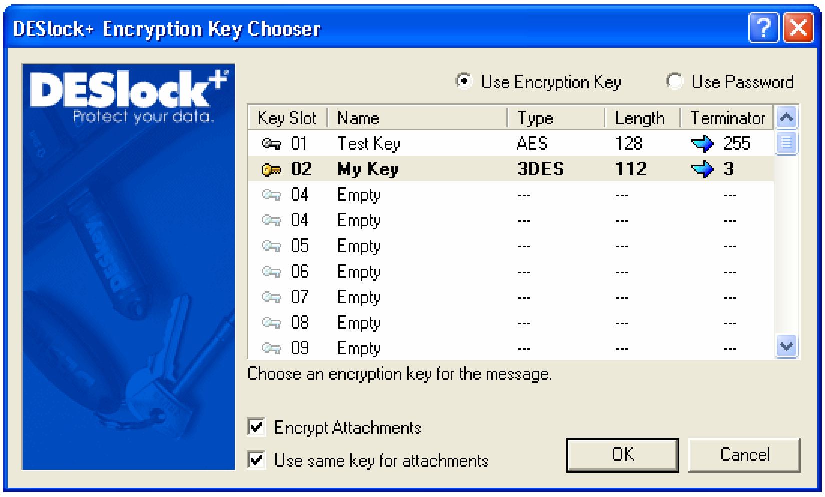
Subject: Top Secret

Attach: Official Report.doc (11 KB)

```
Hi Tom

I have attached the information you wanted.

Dick
```

Figure 15 - 4

After choosing to encrypt the message, an encryption key must be selected or password must be chosen will be used for the encryption of the message (Figure 15 - 5). Any user of DESlock+ can decrypt a message encrypted using a password if they know the password. If an encryption key is used then the recipient must have a copy of that encryption key available to them.



DESlock+ Encryption Key Chooser

● Use Encryption Key ○ Use Password

Key Slot	Name	Type	Length	Terminator
01	Test Key	AES	128	255
02	**My Key**	**3DES**	**112**	**3**
04	Empty	---	---	---
04	Empty	---	---	---
05	Empty	---	---	---
06	Empty	---	---	---
07	Empty	---	---	---
08	Empty	---	---	---
09	Empty	---	---	---

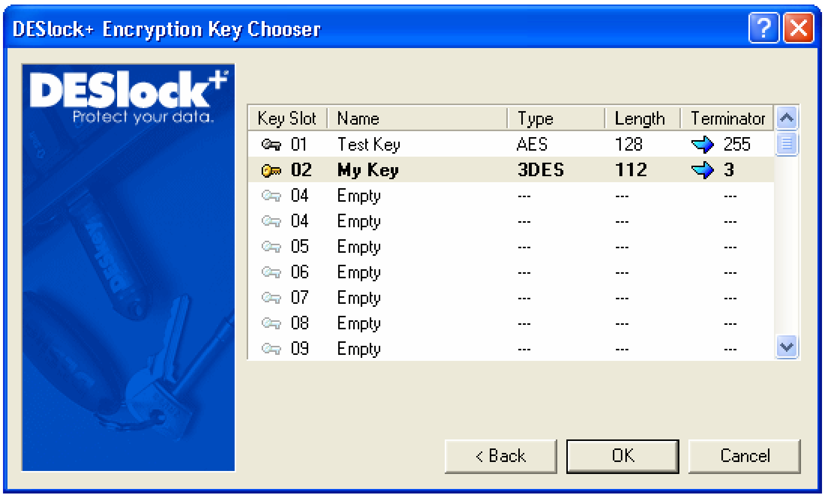
Choose an encryption key for the message.

☑ Encrypt Attachments

☑ Use same key for attachments

Figure 15 - 5

If the message has attachments, the option to select a different encryption key to encrypt the attachments is given. If an alternate encryption key is required, uncheck **Use same key for attachments** and choose a second encryption key on the following screen (Figure 15 - 6). If a password was chosen above, this same password will also be used to encrypt attachments.

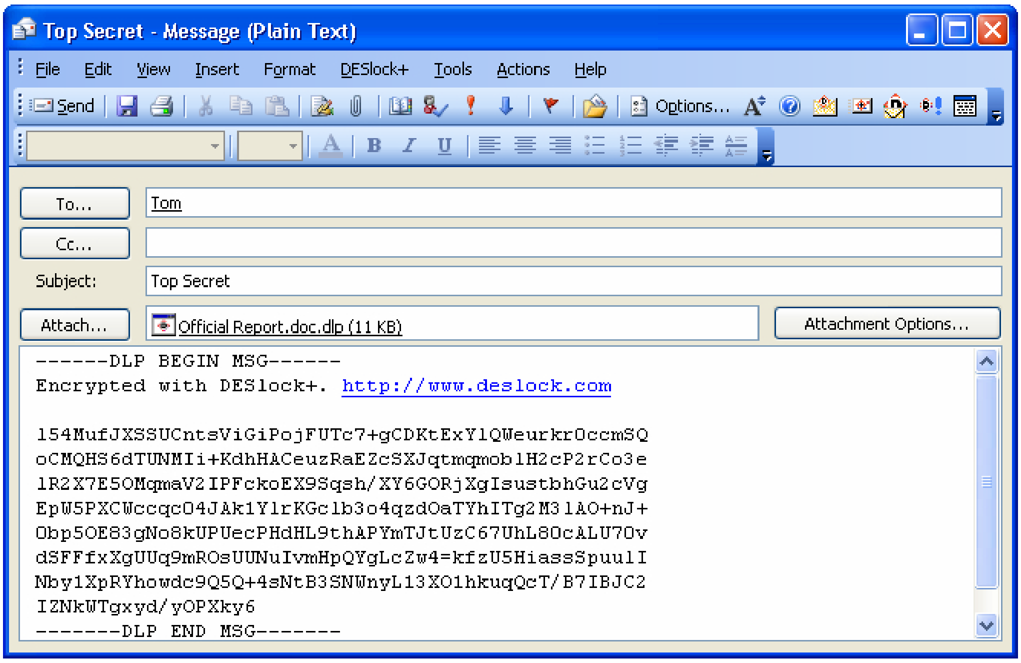


DESlock+ Encryption Key Chooser

Key Slot	Name	Type	Length	Terminator
01	Test Key	AES	128	255
02	**My Key**	**3DES**	**112**	**3**
04	Empty	---	---	---
04	Empty	---	---	---
05	Empty	---	---	---
06	Empty	---	---	---
07	Empty	---	---	---
08	Empty	---	---	---
09	Empty	---	---	---

Figure 15 - 6

Below is the message after encryption. Please note that the message text has been encrypted along with the attachment. We can now add some plain text to be sent along with the encrypted message.


Top Secret - Message (Plain Text)
File Edit View Insert Format DESlock+ Tools Actions Help
Send
Options...
Attachment Options...

To... Tom

Cc...

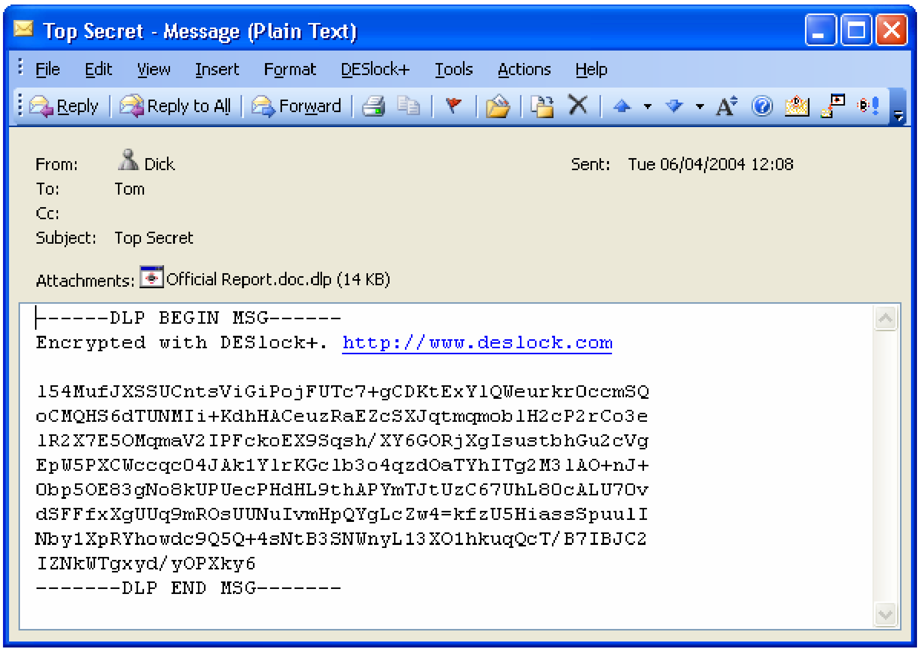
Subject: Top Secret

Attach... Official Report.doc.dlp (11 KB)

```
------DLP BEGIN MSG------
Encrypted with DESlock+. http://www.deslock.com

l54MufJXSSUCntsViGiPojFUTc7+gCDKtExYlQWeurkrOccmSQ
oCMQHS6dTUNMIi+KdhHACeuzRaEZcSXJqtmqmoblH2cP2rCo3e
lR2X7E5OMqmaV2IPFckoEX9Sqsh/XY6GORjXgIsustbhGu2cVg
EpW5PXCWccqcO4JAk1YlrKGclb3o4qzdOaTYhITg2M3lAO+nJ+
Obp5OE83gNo8kUPUecPHdHL9thAPYmTJtUzC67UhL8OcALU7Ov
dSFFfxXgUUq9mROsUUNuIvmHpQYgLcZw4=kfzU5HiassSpuulI
Nby1XpRYhowdc9Q5Q+4sNtB3SNWnyL13XO1hkuqQcT/B7IBJC2
IZNkWTgxyd/yOPXky6
-------DLP END MSG-------
```

Figure 15 - 7

Below is the message as the recipient would see it.


Top Secret - Message (Plain Text)
File Edit View Insert Format DESlock+ Tools Actions Help
Reply
Reply to All
Forward

From: Dick

Sent: Tue 06/04/2004 12:08

To: Tom

Cc:

Subject: Top Secret

Attachments: Official Report.doc.dlp (14 KB)

```
------DLP BEGIN MSG------
Encrypted with DESlock+. http://www.deslock.com

l54MufJXSSUCntsViGiPojFUTc7+gCDKtExYlQWeurkrOccmSQ
oCMQHS6dTUNMIi+KdhHACeuzRaEZcSXJqtmqmoblH2cP2rCo3e
lR2X7E5OMqmaV2IPFckoEX9Sqsh/XY6GORjXgIsustbhGu2cVg
EpW5PXCWccqcO4JAk1YlrKGclb3o4qzdOaTYhITg2M3lAO+nJ+
Obp5OE83gNo8kUPUecPHdHL9thAPYmTJtUzC67UhL8OcALU7Ov
dSFFfxXgUUq9mROsUUNuIvmHpQYgLcZw4=kfzU5HiassSpuulI
Nby1XpRYhowdc9Q5Q+4sNtB3SNWnyL13XO1hkuqQcT/B7IBJC2
IZNkWTgxyd/yOPXky6
-------DLP END MSG-------
```

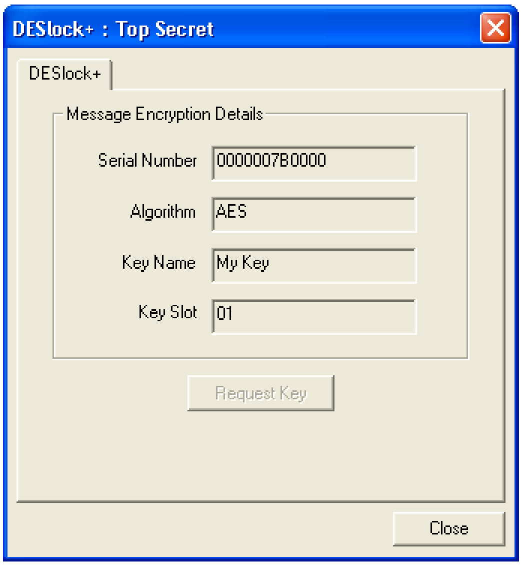
Figure 15 - 8

Depending on the setting used, and assuming the recipient has the correct encryption key, the message can be decrypted in the email window or in the DESlock$^+$ Message Viewer (see page 105).

Message Properties

Selecting **Message Properties** from the **DESlock+** menu will show details of the encryption key used to encrypt any DESlock$^+$ encrypted message. The encryption key serial number and algorithm type will always be displayed. If the encryption key exists within the active DESkey key space, the location (key slot) and key name will also be shown. If the email was encrypted using a password, the text "Uses Password" will be displayed in the Key Name box.

If the encryption key does not exist in the active DESkey key space the option to request the encryption key is given. If the button is clicked an encryption key request email will be generated when the properties dialog is closed. This email will be addressed to the encrypted message originator but this can be changed prior to sending the message if required. The request message can then be sent to the desired user and used by them in the key issue process.



DESlock+ : Top Secret

Message Encryption Details

Serial Number: 0000007B0000

Algorithm: AES

Key Name: My Key

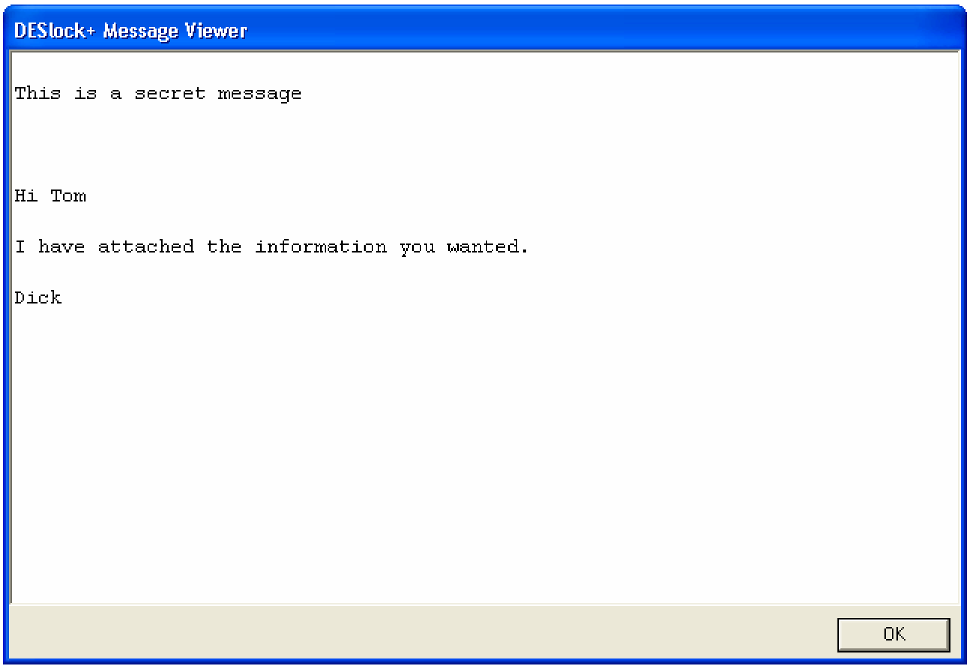
Key Slot: 01

Figure 15 - 9

DESlock$^+$ Message Viewer

The DESlock$^+$ Message Viewer is a simple tool that enables an encrypted message to be viewed securely. When used, DESlock$^+$ will decrypt an encrypted message to the viewer window rather than decrypting the original copy in the email.

The DESlock$^+$ Message Viewer disables any editing of the email including copying the text using Windows clipboard.



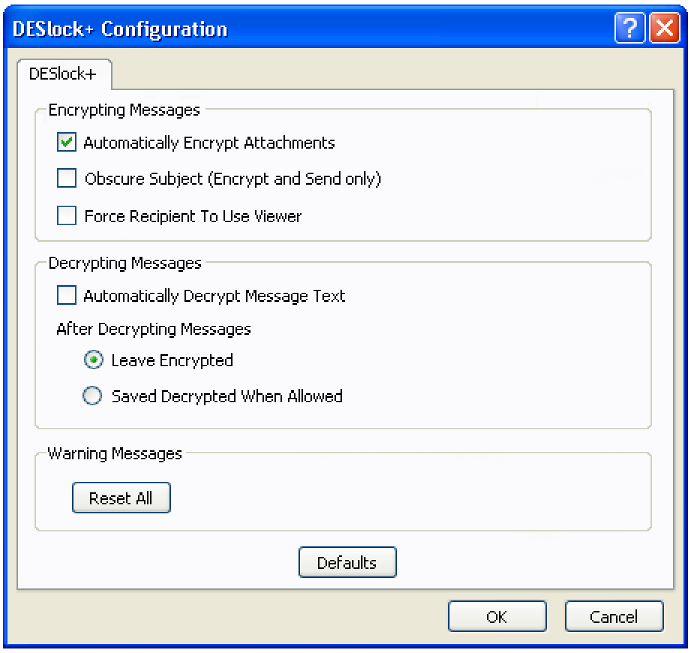
```
This is a secret message


Hi Tom

I have attached the information you wanted.

Dick
```

Figure 15 - 10

Even after the message has been decrypted to the viewer, the original email will remain in the encrypted form. A decrypted copy of the email therefore cannot be forwarded if **Force Viewer** is selected when encrypting the message.

DESlock$^+$ Configuration

Clicking the DESlock$^+$ icon on the toolbar, or selecting Configuration from the **DESlock+** menu, will display the configuration dialog (Figure 15 - 11) which allows control of the default operation of the DESlock$^+$ Outlook Plug-in.



Encrypting Messages

☑ Automatically Encrypt Attachments

□ Obscure Subject (Encrypt and Send only)

□ Force Recipient To Use Viewer

Decrypting Messages

□ Automatically Decrypt Message Text

After Decrypting Messages

● Leave Encrypted

○ Saved Decrypted When Allowed

Warning Messages

Figure 15 - 11

Encrypting Messages

Automatically Encrypt Attachments

If selected, the Plug-in will default to encryption of email attachments when the message body is encrypted.

Obscure Subject (Encrypt and Send only)

If selected, the original subject field of an encrypted email is replaced with the text "A DESlock+ Encrypted Message". The original subject is encrypted and saved with the message and is only visible after decryption.

Force Recipient to Use Viewer

If selected the recipient of the message will be forced to use the DESlock+ message viewer to view the message, regardless of the recipients DESlock+ viewing options.

Decrypting Messages

Automatically Decrypt Message Text

If selected, any DESlock$^+$ encrypted emails will automatically be decrypted when they are opened assuming the correct encryption key is stored within the active DESkey. If not selected, 'Decrypt Now' must be manually selected.

After Decrypting Messages

Select to either always store the message in encrypted format, even if it has been decrypted, or to store the message in decrypted format after it has been decrypted.

Warning Messages

Reset All

If any of the warning message boxes have been previously dismissed with 'do not ask me again', clicking this button will cause all messages to revert to their initial state so will be displayed until dismissed again.

Key Transfer

In addition to encrypting messages and attachments, the Outlook Plug-in also provides Key Transfer integration allowing the entire key transfer process to be performed from within Outlook. Please note this will only work with a DK5 DESkey as a Key-File does not support key transfers. Refer to the Key Transfer Wizard documentation on page 69 for a more detailed overview of the process.

Three additional menu options are available depending on the current stage of key transfer. The menu options are listed below in the order they are shown.

Request Key

To request an encryption key, create a new email message from within Outlook. From the **DESlock+** menu of the message window choose **Request Key**. The message can then be addressed and edited before being sent, at which point a request file will automatically be attached to the email.

Process Key Request

The recipient of the Request email should then choose **Process Key Request** from the **DESlock+** menu of the message window. Selecting this will allow the creation of an issue file based upon the attached request file.

An encryption key to transfer must be selected in the same way they would using the Key Transfer Wizard (described on page 72).

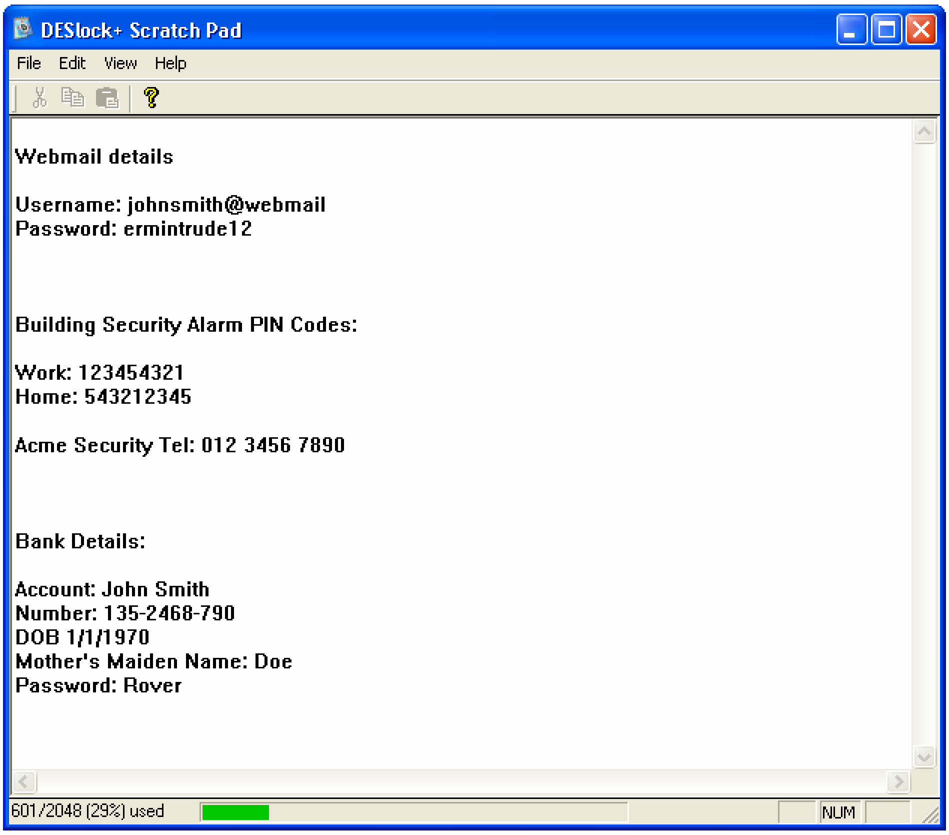
When the encryption key has been specified the Plug-in will create a new email containing the issue file and save it to the 'drafts' folder in Outlook. The user issuing the key must open this email, address it and send it.

Process Key Update

When the user requesting the encryption key receives the update email, they should choose **Process Key Update** from the **DESlock+** menu of the message window. This will allow the encryption key to be added to the DESkey key space (described on page 75).

Scratch Pad

The Scratch Pad (Figure 16 - 1) is a text editor that can be used to write and store information into a secure memory area of the currently active DK5 DESkey. Any data written to the DESkey using the Scratch Pad will be kept in the DESkey until it is deleted by the user. The Scratch Pad editor cannot be used with a DESlock$^+$ Key-File.



Webmail details

Username: johnsmith@webmail
Password: ermintrude12

Building Security Alarm PIN Codes:

Work: 123454321
Home: 543212345

Acme Security Tel: 012 3456 7890

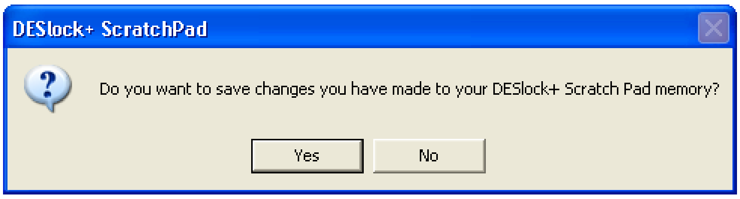
Bank Details:

Account: John Smith
Number: 135-2468-790
DOB 1/1/1970
Mother's Maiden Name: Doe
Password: Rover

601/2048 (29%) used

Figure 16 - 1

If the Scratch Pad data has been modified and an attempt to close the scratch pad is made, the dialog box below (Figure 16 - 2) will be shown, allowing the user to save the modified data to the DESkey before exiting. If the scratch pad data does not need to be updated, scratch pad will be closed normally.



Do you want to save changes you have made to your DESlock+ Scratch Pad memory?

Figure 16 - 2

As a security feature, Scratch Pad data is secure and cannot be copied to the Windows clipboard unless the "Use Windows Clipboard" is selected in the Edit menu.