Cipherlok™

Cipherlok™ Manual

This document is provided by Softlok International Ltd for informational purposes only to licensed users of the Cipherlok product and is provided on an ‘as is’ basis without any warranties expressed or implied.

Other names are trademarks or registered trademarks of the respective holders. Microsoft is a registered trademark and Windows, Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP and their respective logos are registered trademarks of the Microsoft Corporation.

Information in this document is subject to change without notice and does not represent a commitment on the part of Softlok International Ltd. The software described in this document is provided under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software except as specifically allowed in the license.

It is the users responsibility to ensure the suitability of Cipherlok before using it. In no circumstances will Softlok International Ltd be responsible for any loss or damage of data or programs as a result of using Cipherlok. We strongly suggest that the user keep multiple copies of any Cipherlok USB Tokens used for encryption or store securely the passphrase used for encryption. Failure to do so may result in the permanent loss of data. Your use of Cipherlok implies acceptance of these terms.

Contents

Chapter 1 Introduction

What is Cipherlok?

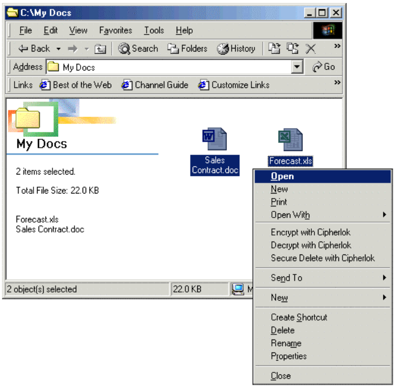
Cipherlok is a simple to use yet highly secure way to encrypt files on your computer. Once encrypted using Cipherlok's 160 bit key and Blowfish algorithm files are virtually impossible to crack even given complete access to the computer.

To provide a higher level of security and simplify use Cipherlok has been designed to work with Cipherlok USB Tokens that contain the passphrase used for encryption and decryption. However it can also work with manually typed passphrases.

There are many applications for Cipherlok but one of the most important is that users of notebook computers can encrypt files while travelling to ensure confidential documents are completely safe if stolen.

How does it work?

Cipherlok can be used to encrypt files directly wherever Windows explorer is used. Simply right click the selected files or folders and click *Cipherlok Encrypt*.



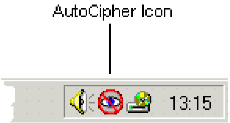
2 items selected.

Total File Size: 22.0 KB

Forecast.xls
Sales Contract.doc

If a USB token is connected then the files will be encrypted. If not you will first be asked for a passphrase to use. This right click menu is also available in the *Open* and *Save As* dialog boxes of most applications.

If there are certain files that are regularly encrypted then AutoCipher can be used to automatically decrypt them at startup and ensure they are encrypted at shutdown. This way the files are ready to use when you need them but secured when your PC is shutdown or you have logged off without the delays associated with secure filing systems. AutoCipher is a system tray application and if enabled the icon will appear on the task bar.


AutoCipher Icon

System Requirements

The Cipherlok software will work on any PC running Windows 95, 98, ME, NT4, 2000 or XP and having 3MB of free hard disk space. Use of the hardware Cipherlok tokens requires Windows 98, ME, 2000 or XP and a USB port.

Installation

To install Cipherlok simply run setup.exe and follow the instructions. If you are installing on Windows NT, 2000 or XP then you must have administrator privileges to run setup. After installation a new Cipherlok entry will appear in the Start menu with links to Cipherlok Settings and Cipherlok Token Wizard. Cipherlok encrypt, decrypt and secure delete options are also added to the Windows explorer right click menu. Cipherlok AutoCipher may also appear in the system tray area if enabled.

Trial Version

When first installed Cipherlok will work unrestricted for 30 days allowing you to evaluate it. The only difference with the registered version is that you probably don’t have a USB token so you will have to enter passphrases by typing them. After the 30 day trial period the encrypt and secure delete functions will be blocked until registration. You will still be able to decrypt any files encrypted during the trial period though.

Registration

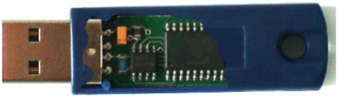
To register Cipherlok select the Register item from the Windows explorer right click menu or the Register tab of the Cipherlok Settings program. Make a note of the serial number which you will need when registering at www.softlok.com.

Registering entitles you to 1 year of free software updates and technical support. An unlock key will be sent by email and the tokens (where required) shipped the same day.

Chapter 2 Using Cipherlok

Encrypting with a USB Token

Cipherlok USB Tokens are supplied by us blank so before you can use them they must be programmed. See how to do this in Chapter 3 – Tokens Wizard.



Cutaway picture of the Cipherlok USB Token

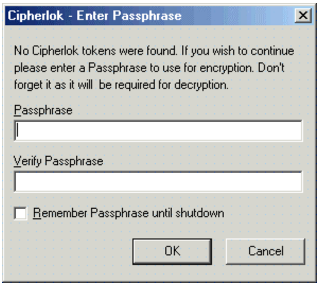
To encrypt a file, folder or selection simply highlight them, right click on the mouse and click Cipherlok Encrypt. Cipherlok will then search for a USB token to provide the passphrase. If no PIN is required by the token then encryption will begin. If a PIN is required then this will need to be entered correctly first. After encryption the file will have the extension .cip and will display the Cipherlok icon. e.g, if you encrypt the file readme.txt it will be called readme.txt.cip. Decryption works exactly the same way – it is that simple!

If more than one USB token is connected to the PC when you wish to encrypt or decrypt then a dialog box will appear asking you to choose which token to use. If you try to decrypt files with the wrong token then Cipherlok will report the number of files that could not be decrypted correctly.

Remember that Cipherlok works like other features of Windows Explorer. For instance if you select a folder Cipherlok will encrypt all of the files and subfolders within it automatically. Cipherlok does try to stop you from encrypting the Windows folder or system files but you must still be careful. You have been warned!

Encrypting with a passphrase

Although designed to work best with USB tokens Cipherlok can still be used with traditional passphrases as well. If no token is found when encrypting or decrypting then you will be requested to type the passphrase. During encryption you must enter the passphrase twice for safety.



Cipherlok - Enter Passphrase

No Cipherlok tokens were found. If you wish to continue please enter a Passphrase to use for encryption. Don't forget it as it will be required for decryption.

☐ Remember Passphrase until shutdown

Do not forget it otherwise the files will not be retrievable. By default the passphrase will have to be entered each time you encrypt or decrypt files but you can if you wish click the ‘Remember Passphrase’ checkbox which will remember the passphrase until shutdown or earlier if you request Cipherlok to erase it. It is stored only in memory and not saved to a file but this may still reduce the security of the system. To force Cipherlok to erase a stored passphrase select the option from the Windows Explorer right click menu or the AutoCipher right click menu on the system tray (see AutoCipher for more details).

Remember that Cipherlok works like other features of Windows Explorer. For instance if you select a folder Cipherlok will encrypt all of the files and subfolders within it automatically. Cipherlok does try to stop you from encrypting the Windows folder or system files but you must still be careful. You have been warned!

Secure file deletion

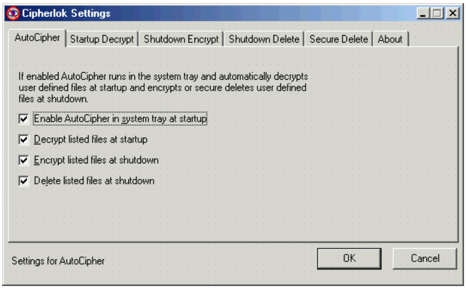
If Cipherlok simply encrypted a file and deleted the original then the security would be weak as deleted files can often be undeleted. To solve this problem Cipherlok first overwrites the original file with a pattern of 0’s and 1’s a certain number of times before deleting it. This makes it virtually impossible to retrieve the file. By default this is done twice which should be sufficient for most applications but this can be changed from the Cipherlok Settings program on the *Secure Delete* tab. The NSA recommend a setting of 7 for highly confidential documents but this will slow down the encryption process and would only be required in extreme circumstances.

As the secure deletion of files is of such importance to a secure environment we decided to make this option separately available on the right click menu so that you can delete files that are no longer required.

Cipherlok AutoCipher

Overview

AutoCipher is a background system tray program that can automatically decrypt certain files at startup and encrypt or secure delete files at shutdown. If AutoCipher is enabled then you will see the icon in the system tray section of the task bar. To enable and setup AutoCipher you need to run the Cipherlok Settings program.



If enabled AutoCipher runs in the system tray and automatically decrypts user defined files at startup and encrypts or secure deletes user defined files at shutdown.

☑ Enable AutoCipher in system tray at startup

☑ Decrypt listed files at startup

☑ Encrypt listed files at shutdown

☑ Delete listed files at shutdown

Settings for AutoCipher

First check that it is enabled on the AutoCipher tab. There are three other tabs used by AutoCipher – *Startup Decrypt, Shutdown Encrypt and Shutdown Delete*. Each tab has a file list where you can drag files or folders. By default files added to the encrypt at shutdown list will also be added to the decrypt at startup list but you can uncheck the box if you don’t want this. Be careful if you add any files to the delete at shutdown list as they will be deleted next time you shutdown or logoff and will not be recoverable.

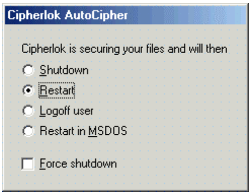
AutoCipher is fully compatible with multi user systems. Each Windows user has their own list of files to decrypt at startup, encrypt at shutdown and delete at shutdown. Each user can also enable or disable AutoCipher as required.

AutoCipher in use

The most effective way to use AutoCipher is with a USB Cipherlok Token. Just ensure that the token is plugged in before starting up your PC and leave it there until you logoff or shutdown. Then remove the token and keep it somewhere safe.

During startup AutoCipher will attempt to decrypt all of the files and folders listed in the *Startup Decrypt* file list. It will try to do this first with a USB token but if none is found then it will request a passphrase.

When you attempt to shutdown your PC or notebook AutoCipher will begin to secure your files. First it will ensure that all files and folders listed in the *Shutdown Encrypt* file list are encrypted. Secondly it will secure delete all of the files and folders listed in the *Shutdown Delete* file list. While doing this it will display a small dialog box explaining what kind of shutdown it will perform after it has finished.



Cipherlok AutoCipher

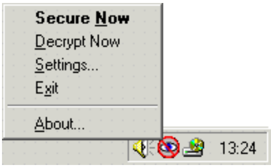
Cipherlok is securing your files and will then

○ Shutdown
● Restart
○ Logoff user
○ Restart in MSDOS

☐ Force shutdown

Normally this shutdown type (shutdown, restart, logoff, restart in msdos mode) will be as you requested so you don't have to do anything. However there could be times when AutoCipher cannot determine whether you wish to shutdown or restart so you can change what it has decided to do by clicking the appropriate button before it finishes. One other feature of the shutdown dialog box is that it has a *Force shutdown* checkbox. This is useful if you have any applications that don't close properly and will force them to close.

Popup menu



AutoCipher has a popup menu that can be accessed by right clicking the icon. From the menu you can immediately secure your PC by selecting *Secure Now*. This will perform the same functions as at shutdown without actually shutting down and will also erase any stored passphrase in memory. This is useful if you have to leave your PC unattended for a while. This *Secure Now* feature can also be activated by simply double clicking the AutoCipher icon. *Decrypt Now* will decrypt files as at startup. *Erase Passphrase* will erase any stored passphrase from memory. Selecting *Settings* will open up the Cipherlok Settings program.

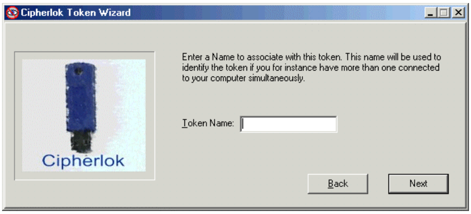
Chapter 3 Token Wizard

Programming Cipherlok USB Tokens

Cipherlok USB Tokens are supplied from us blank to ensure your security. Before you can use them you need to program them using the Cipherlok Token Wizard which can be run from the Windows Start menu. If your version of Windows does not support USB then the wizard will not have been installed. Supported versions of Windows are 98, ME, 2000 and XP.

The first page of the wizard just explains what it is going to do so just click *Next*.

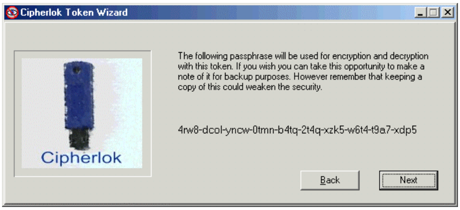
The first information the wizard will request is a token name. This name is required to identify the token if more than one are connected at the same time. In most cases just enter your first name and click *Next*.



Enter a Name to associate with this token. This name will be used to identify the token if you for instance have more than one connected to your computer simultaneously.

Token Name:

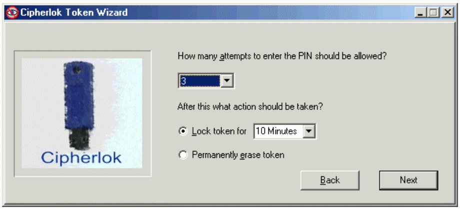
The next detail requested is the passphrase to use for encryption and decryption. You can enter a passphrase that you wish to use containing up to 64 characters (not case sensitive). However we recommend that you leave it blank and just click *Next* to have a random one generated. If you do this the next page will display the random passphrase chosen and you can keep a record of it for emergency use if you wish.



The following passphrase will be used for encryption and decryption with this token. If you wish you can take this opportunity to make a note of it for backup purposes. However remember that keeping a copy of this could weaken the security.

4rw8-dcol-yncw-0tmn-b4tq-2t4q-xzk5-w6t4-t9a7-xdp5

The next page asks whether you wish to protect use of the token using a PIN. This PIN will be requested each time the token is used to encrypt or decrypt a file and can be useful to stop a colleague who has access to your PC. Leave it blank and click *Next* if you don't need this feature. If required enter a PIN from 3 to 8 numeric digits (e.g. 7235) and click *Next*. You can now select how many times a PIN can be incorrectly entered and what action will be taken if this happens. For instance you may decide to allow the wrong PIN to be entered an unlimited number of times or to lock the token from use for 30 minutes after 3 attempts. The choice is your and depends on the application. One other feature is that you can have the entire token erased after the wrong PIN has been entered more than allowed. This is an extreme measure but could be useful in some circumstances.



How many attempts to enter the PIN should be allowed?

3

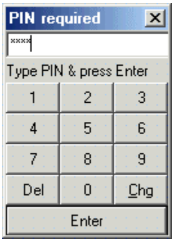
After this what action should be taken?

● Lock token for 10 Minutes

○ Permanently erase token

The final step of the wizard is to program the tokens. Just plug in a token (only one at a time) and click the *Program* button. We recommend that you program at least two with a particular passphrase and keep one in a safe place. This protects you against loss, theft or damage of a token.

The PIN dialog box



Whenever you attempt to use a token that has a PIN defined you will see the PIN dialog box. You should enter the required PIN and then click the *Enter* button. If you wish to change the PIN then enter it but instead of clicking *Enter* click *Chg*. You will then need to enter the new PIN twice for confirmation.

Whenever you enter a wrong PIN an error will be displayed. After you have entered the wrong PIN more than allowed the token will be locked for a defined time or will be erased permanently. If the token is locked the time will only elapse while the PIN dialog box is displayed. If the dialog is closed the token will remember the remaining time still to be locked – there is no way round this! The Cipherlok token will also report that it has detected somebody trying to guess the PIN each time it is used.

Chapter 4 Frequently asked questions

How can I encrypt all files containing a certain keyword?

The simplest way to do this is to use the Windows search feature and search for all files (*.*) containing the text ‘your keyword’. When the search is complete simply select all of the files found, right click and select *Cipherlok Encrypt*. You can also drag the files found to the *Shutdown Encrypt* tab of Cipherlok Settings if you wish to always keep these files secure. Remember Cipherlok works wherever Windows explorer is used which includes most open file and save-as dialog boxes and the Windows search utility.

What does AutoCipher do when I logoff instead of shutdown?

AutoCipher handles a logoff in the same way as shutdown and will secure the required files. However Windows XP has a new feature called ‘Switch Users’ which allows a user to switch to another user account while leaving all open files and applications available to the new user. In this case AutoCipher will not secure files as Windows has not technically logged off the user. You can however double click the AutoCipher icon any time to secure the files before switching users.

Does Cipherlok handle shortcut files?

Cipherlok will attempt to encrypt the file pointed to by a shortcut file rather than encrypt the shortcut file itself. It will also attempt to change the filename pointed to with the extension .cip. However Windows has some strange anomalies meaning that this sometimes does not work leaving the shortcut pointing to the original filename that Windows thinks doesn’t exist. We recommend not encrypting shortcut files although doing so should not cause any damage to the files.

Why is decryption much faster than encryption?

After encrypting a file Cipherlok needs to secure delete the original file to ensure it cannot be retrieved. This process takes time depending on how many times Cipherlok has to overwrite the file. This setting is defined on the *Secure Deletion* tab of Cipherlok Settings. When decrypting, the original file can be simply deleted, as it was encrypted anyway, reducing the time taken.

Can Cipherlok encrypt files on floppy disks or memory cards?

Yes Cipherlok can work with these media but it requires free space on the device equal to the size of the largest file to be encrypted. This is because Cipherlok keeps a copy of the original file during encryption to safeguard against a power interruption or system crash.

Is there a way we can access the Cipherlok encryption and decryption features from our own application?

It is possible to use Cipherlok from your own application to automate the secure access to database files for example. Please contact us for further details if you require this.