MessageLock User's Manual

MessageLock Overview

Installing and Uninstalling

Installing and Uninstalling

If you are reading this text, then MessageLock is installed on your computer.

How To Reinstall MessageLock
To reinstall MessageLock, you must first uninstall it completely. To accomplish this:
-Exit Microsoft Outlook.
-Go to Start>Control Panel>Add/Remove Programs.
-Select MessageLock from the list and follow the Windows prompts to uninstall.

Before running the MessageLock installer, be certain that Microsoft Outlook is not loaded.

Uninstalling MessageLock
MessageLock, you must first uninstall it completely.
To do this exit Microsoft Outlook. Go to Start>Control Panel>Add/Remove Programs. Select MessageLock from the list and follow the prompts.

Exporting Your Passwords
Prior to uninstalling MessageLock, we encourage you to export your passwords so that you can continue to access files on your computer that were encrypted with AES-256, AES-128 and Zip 2.
To export Passwords, go to Outlook's Tools menu, and select MessageLock. This brings up the MessageLock Preferences screen. Next, select the Encryption Tab, then Encryption Settings. Select the Export Passwords button and follow the prompts.

System Requirements

System Requirements

Before installing MessageLock, be certain that your computer meets the following minimum software and hardware requirements.

Requirement	
Operating System and Requirements	Windows 2000 Professional, Windows XP Home, or Windows XP Professional. Microsoft .NET Framework 2.0
Software	Microsoft Outlook 2000/XP/2003/2007/2010 (32 bit), with latest service packs installed.
Processor	Pentium class Recommended: Pentium 4-class. Minimum processor speed 600 MHz
RAM	Recommended: minimum of 256 MB
Available Hard Disk Space	50 MB free disk space on the installation drive

Getting Started

Getting Started with MessageLock

Practical email encryption using zip compatible AES encryption.

We hope you'll find MessageLock(TM) by Encryptomatic(TM) to be an invaluable tool to help you achieve your privacy goals.

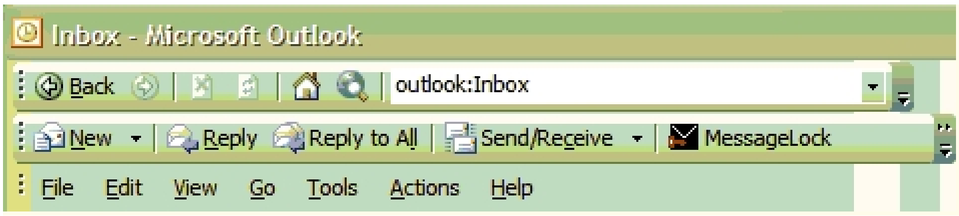
What is Does

MessageLock® is a add-in for Outlook (2000/XP/2003/2007/2010 32bit) that lets you:

- Compress outbound email file attachments, thus saving hard disk space and bandwidth
- Open inbound zip file attachments.
- Send encrypted email messages in a widely compatible format.

MessageLock's primary purpose is to protect your email and/or attachments with strong AES encryption. Encryption is applied on the workstation, protecting your message from the moment it leaves your computer.

A great deal of flexibility has been built into MessageLock. You can control MessageLock's settings from the setup screen, which is accessible from the main Outlook toolbar. To access settings, click on the MessageLock button.



3 Step Quick Start

1. Agree on a password with someone that you want to exchange email messages with. We do not recommend that you do this via email. Use a separate communication channel, such as a face-to-face meeting, telephone, or even instant messenger.
2. Type an email message addressed to the recipient.
3. Click the "Encrypt Email" button and press Outlook's "Send" button. If this is the first time that you have sent an encrypted message to this person, MessageLock will prompt you for a password, and can optionally store the password for future use. The next time you send an encrypted email to this address, MessageLock will recall the stored password and use it to encrypt the message. This password can be changed by you at any time..

Key Features

Key Features

MessageLock can be configured to behave according to the needs and preferences of the user.

MessageLock's key features are:

1. Processing zip files attached to inbound emails
2. Compressing outbound attached files into a zip file
3. Encrypting outbound file attachments
4. Encrypting outbound email messages

Out of the box, MessageLock's default settings are:

Outbound File Compression default is on
Outbound File encryption default is off
Outbound Message encryption default is off
Inbound File Decompression is off
Inbound file and message decryption is on

Encryption Methods

Understanding Encryption Methods

The encryption preferences tab is where you enter individual email addresses, along with an inbound password and an outbound password. These passwords can be the same, or different, depending on your personal preference. We recommend using separate passwords for sending and receiving, as it enhances security.

MessageLock supports several standard encryption methods, including Advanced Encryption Standards (AES) also known as Rijndael. AES has been adopted by the U.S. Government as an encryption standard. The specifications for the Rijndael standard may be downloaded from the NIST by following this link.

MessageLock supports the WinZip™ method of implementing encryption, which encrypts the individual documents within a zip file. Although the documents are encrypted, the names of the documents are visible, as is size of the documents. Supporting the WinZip™

AES implementation means that MessageLock protected files may be accessed by people who know the password, but who do not have MessageLock installed; all that is required is a standard zip utility that supports AES or Zip2.0 encryption. A good free zip utility that supports AES encryption is TugZip. WinZip™ 9.0 and 10.0, and the latest PKZip also support AES, but are not free.

MessageLock has implemented the following AES methods:

AES 128 is 128-bit encryption, much stronger than Zip2.0, and widely compatible. Secure, and not known to have ever been cracked. Using this method encrypts the individual files residing within the Zip container file.

AES 256 is very strong 256-bit encryption, but less compatible. Very secure and not known to have ever been cracked. Using this method encrypts the individual files residing within the Zip container file.

ML-AES 256 is MessageLock's own implementation of AES256 and is not compatible with any Unzip utilities. ML-AES256 encrypts the entire zip container using AES-256 encryption, so that the names of the files can not be viewed. This provides an added level of protection over the WinZip™ method, as no clues about the importance of the contents may be seen.

Zip 2.0. For backwards compatibility, MessageLock implements the old Zip2.0 compression. This is weak encryption but also the most universally compatible with older unzip utilities. Although using weak Zip 2.0 is still much better than not using any encryption, and though it still requires a significant effort to crack, it is not recommended as a default encryption method because it has been cracked.

Selecting an Encryption Method

Message Lock will allow you to set the default encryption standard from its Encryption Settings Tab.

You may override the default encryption standard each time you enter an email address and password on the an email address or password in the Manage Password screen

Use MessageLock's random password generator for creating strong outbound passwords. Just place the cursor in the password field and click on the circular icon to the left of the field.

These passwords must be shared with the other party. We do not recommend that you send passwords in email. Use another communication channel for sharing passwords.

If both parties are using MessageLock, the process of encrypting and decrypting files is virtually transparent. When an encrypted message is received, MessageLock will automatically check its password database. If it finds a password associated with the encrypted message, it will attempt to decrypt and automatically restore the message to Microsoft Outlook. MessageLock places a one line tag to the bottom of all messages that it decrypts, so that you'll know that the message was sent to you securely.

Configuring Preferences

Configuring Your MessageLock Preferences

MessageLock's default behavior can be tailored to your specific preferences or needs. The following paragraphs explain the function of the various options.

Access MessageLock's preferences from the MessageLock Option's toolbar on Outlook's main menu.

Compress all outbound attachments

Selecting this box tells MessageLock that you want it to compress all outbound attachments. This means that every time you have file attached to an email, MessageLock will attempt to compress it.

This feature is overridden by the settings under the compress settings tab.

Decompress all inbound attachments

Selecting this box tells MessageLock that you want to automatically decompress (or Unzip) attachments that you receive from others.

Ask for a password if none has been set

Selecting this box tells MessageLock to prompt you for a password if one has not already been associated with an email address.

Automatically decrypt inbound attachments

Selecting this box tells MessageLock to attempt to automatically decrypt an inbound email attachments that have been encrypted.

Compression Settings Preferences

From the Compression Settings preferences window you can access options that will influence how MessageLock will handle inbound and outbound files.

Compression Tab

From here you may select the default compression method, either Zip or Tar. Zip is recommended for Windows computer users.

Advanced Options

You may deactivate any of the other three tabs if they are not relevant to how you want MessageLock to behave.

By checking the tab “Do not compress files smaller than __ KB” you are telling MessageLock not to bother compressing small files. You may set the file size threshold here, and MessageLock will not attempt to compress files that are smaller than your minimum threshold.

Excluded File Extensions Tab

If you do not want MessageLock to attempt to compress certain types of files, such as .zip files which are already compressed, you may specify those file types here.

If a file extension is not listed here, then MessageLock will attempt to compress that file.

Note that if encryption is enabled for a message, then MessageLock disregards this list. MessageLock will bundle all files into a single .zip file, and will then encrypt it.

Excluded Addresses Tab

Email addresses listed here will never be sent a compressed or encrypted file by MessageLock.

Excluded Domains Tab

Email addresses at internet domains that are listed here will never be sent a compressed or encrypted file by MessageLock.

Exception: MessageLock will attempt to compress and encrypt files for a particular email address at an excluded domain IF a password has been entered under the Encryption Preferences for that email address.

Encryption Preferences

The encryption preferences tab is where you can enter individual email addresses, along with an inbound password and an outbound password.

MessageLock supports several standard encryption methods, including Advanced Encryption Standards (AES) also known as Rijndael. AES has been adopted by the U.S. Government as an encryption standard. The specifications for the Rijndael standard may be downloaded from the NIST by following this link.

MessageLock supports the WinZip™ method of implementing encryption, which encrypts the documents within a zip file. Although the documents are encrypted, the names of the documents are visible, as is size of the documents. Supporting the WinZip™ AES implementation means that MessageLock protected messages may be accessed by people who do not have MessageLock installed; all that is required is a standard zip utility that supports AES or Zip2.0 encryption. A good free zip utility that supports AES encryption is TugZip. WinZip™ 9.0 and 10.0, and the latest PKZip also support AES, but are not free.

Here is a description of the MessageLock implemented AES methods:

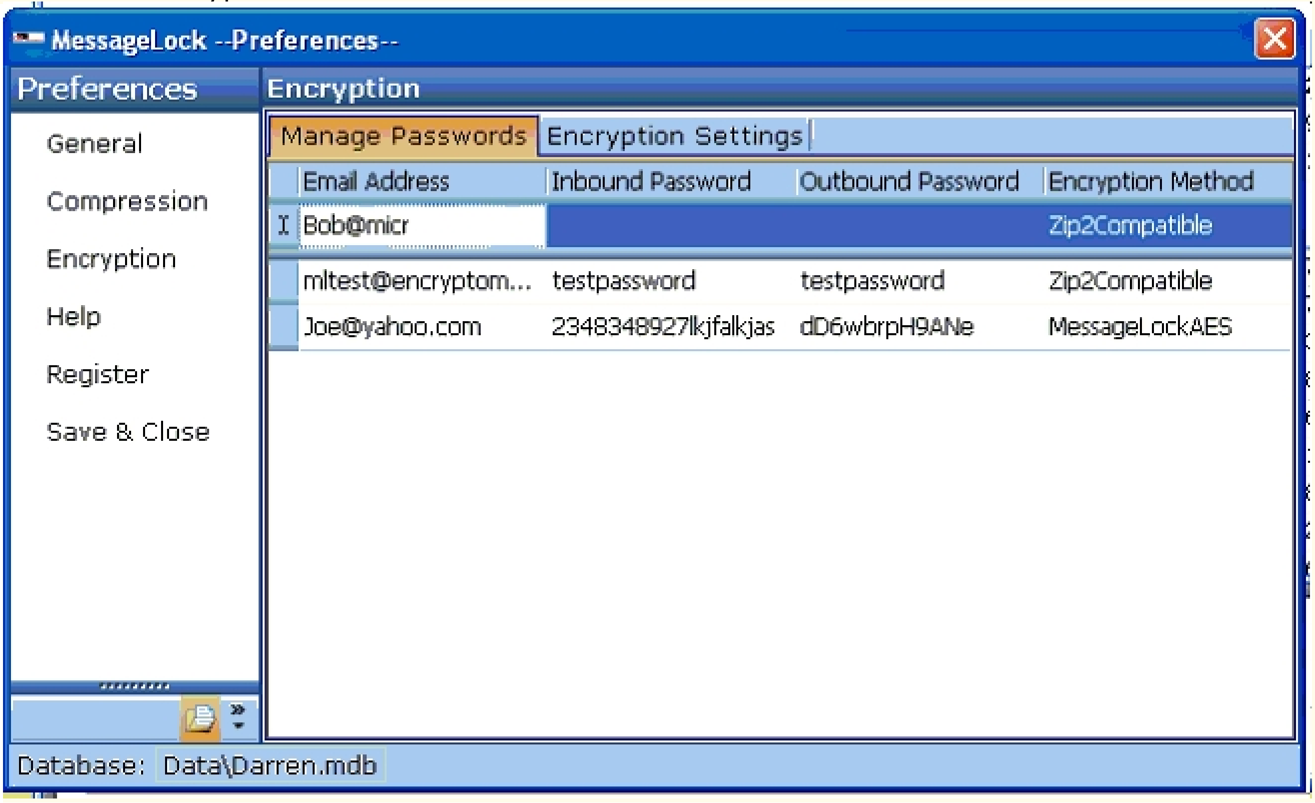
Zip2.0 compression is the weakest, but most universally compatible with older unzip utilities. It is known to be weak encryption and has been cracked.

AES 128 is 128-bit encryption, much stronger than Zip2.0, and widely compatible. Secure, and not known to have been cracked.

AES 256 is very strong 256-bit encryption, but less compatible. Very secure and not known to have been cracked.

ML-AES256 is MessageLock's own implementation of AES256 and is the least compatible method. ML-AES256 encrypts the entire zip container using AES- 256 encryption, so that the names of the files can not be viewed. This provides an added level of protection over the WinZip™ method, as no clues about the importance of the contents may be seen.

To enter an email address or password in MessageLock, simply place the cursor in the text field, and type the email address, the inbound password (the password they use to send to you) and the outbound password (the password you use to send to this email address), and then select the encryption method you wish to use. Now whenever you send to this email address, MessageLock will automatically use this password and encryption method.



Email Address	Inbound Password	Outbound Password	Encryption Method
Bob@micr			Zip2Compatible
mltest@encryptom...	testpassword	testpassword	Zip2Compatible
Joe@yahoo.com	2348348927lkjfalkjas	dD6wbrpH9ANe	MessageLockAES

Database: Data\Darren.mdb

Use MessageLock's random password generator for creating strong outbound passwords. Just place the cursor in the password field and click on the circular icon to the left of the field.

Notice that we have chosen not to obscure your passwords in Microsoft Outlook, so as to facilitate ease of use. The purpose of MessageLock is not to protect data on your PC – there is functionality in Windows that can do a more effective job of that. Rather, MessageLock's purpose is to help protect your email message and attached files while they are in transit across the internet.

These passwords must be shared with the other party. We do not recommend that you send passwords in email. Use another communication channel for sharing passwords.

If both parties are using MessageLock, the process of encrypting and decrypting files is virtually transparent. When an encrypted message is received, MessageLock will automatically check its password database. If it finds a password associated with the encrypted message, it will attempt to decrypt and automatically restore the message to Microsoft Outlook. MessageLock places a one line tag to the bottom of all messages that it decrypts, so that you'll know that the message was sent to you securely.

Credits

Credits

Thank you to our dedicated programming and QA staff, to our enthusiastic beta testers, and to our customers.

Restricted File Attachments

Managing Restricted File Attachments

As a security precaution, Outlook restricts access to certain file attachment types (see below for a list). Microsoft calls these **"Level One"** file types. More information on Outlook restricted file types was available at this web page at the time this was written.

If MessageLock were to automatically or manually extract a Level One file type to Outlook 2003, Outlook would permanently block access to the file. Therefore, MessageLock must treat zip files that contain Level One file types differently than zip files that do not.

When a Zip file is received, MessageLock will always test the file to determine if any of these Outlook-restricted file attachments are inside the zip file, or if the file contains an embedded file directory. If either of these tests are true, then MessageLock will not attempt to unzip the file attachment.   The zip file will remain attached to your email.

You may access Level One files inside of an Outlook email zip file attachment two ways:

First, you could use the MessageLock "Item Viewer" on the email toolbar to manage the file attachment. If Level One file types or a file directory are present in the zip file, the Item Viewer will only allow you to extract the files to a location on your hard disk, and will not allow you to attach the files to the email. If the files in the zip attachment have been encrypted, MessageLock will attempt to locate a stored password in your password list. If no password is found, you will be prompted to enter one.

Secondly, you could right click on the zip file attachment, select "Save As," and save the file to a location on your hard disk. You could then access the file using your system's default Zip utility, such as TugZip or WinZip. If the files in the zip attachment have been encrypted, your zip utility will prompt you to enter a password.

Level One File Types

extension	File type
.ade	Access Project Extension (Microsoft)
.adp	Access Project (Microsoft)
.app	Executable Application
.asp	Active Server Page
.bas	BASIC Source Code
.bat	Batch Processing
.cer	Internet Security Certificate File
.chm	Compiled HTML Help
.cmd	DOS CP/M Command File, Command File for Windows NT
.com	Command
.cpl	Windows Control Panel Extension (Microsoft)
.crt	Certificate File
.csh	csh Script
.exe	Executable File
.fxp	FoxPro Compiled Source (Microsoft)
.hlp	Windows Help File
.hta	Hypertext Application
.inf	Information or Setup File
.ins	IIS Internet Communications Settings (Microsoft)
.isp	IIS Internet Service Provider Settings (Microsoft)
.its	Internet Document Set, Internation Translation
.js	JavaScript Source Code
.jse	JScript Encoded Script File
.ksh	UNIX Shell Script
.lnk	Windows Shortcut File
.mad	Access Module Shortcut (Microsoft)
.maf	Access (Microsoft)
.mag	Access Diagram Shortcut (Microsoft)

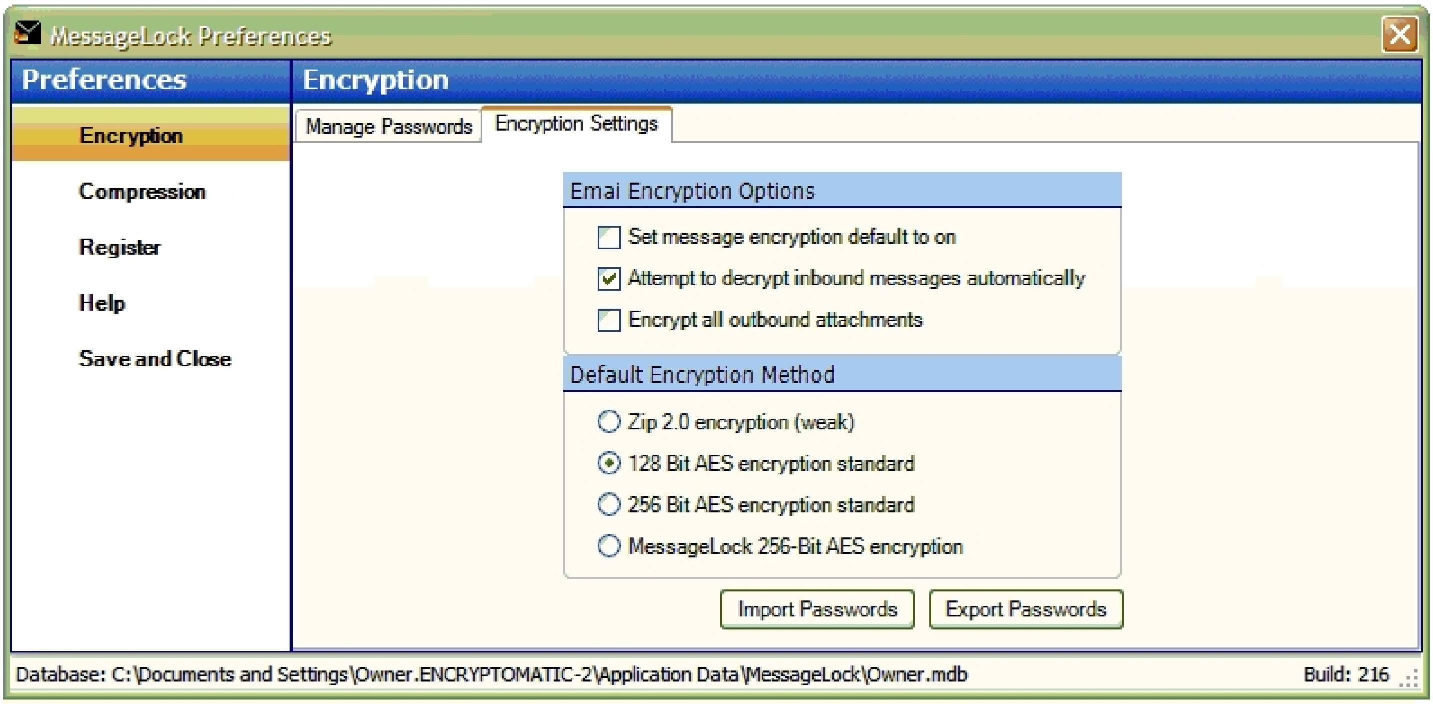
.mam	Access Macro Shortcut (Microsoft)
.maq	Access Query Shortcut (Microsoft)
.mar	Access Report Shortcut (Microsoft)
.mas	Access Stored Procedures (Microsoft)
.mat	Access Table Shortcut (Microsoft)
.mau	Media Attachment Unit
.mav	Access View Shortcut (Microsoft)
.maw	Access Data Access Page (Microsoft)
.mda	Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft)
.mdb	Access Application (Microsoft), MDB Access Database (Microsoft)
.mde	Access MDE Database File (Microsoft)
.mdt	Access Add-in Data (Microsoft)
.mdw	Access Workgroup Information (Microsoft)
.mdz	Access Wizard Template (Microsoft)
.msc	Microsoft Management Console Snap-in Control File (Microsoft)
.msi	Windows Installer File (Microsoft)
.msp	Windows Installer Patch
.mst	Windows SDK Setup Transform Script
.ops	Office Profile Settings File
.pcd	Visual Test (Microsoft)
.pif	Windows Program Information File (Microsoft)
.prf	Windows System File
.prg	Program File
.pst	MS Exchange Address Book File, Outlook Personal Folder File (Microsoft)
.reg	Registration Information/Key for W95/98, Registry Data File
.scf	Windows Explorer Command
.scr	Windows Screen Saver
.sct	Windows Script Component, Foxpro Screen (Microsoft)
.shb	Windows Shortcut into a Document
.shs	Shell Scrap Object File
.tmp	Temporary File/Folder
.url	Internet Location
.vb	VBScript File or Any VisualBasic Source
.vbe	VBScript Encoded Script File
.vbs	VBScript Script File, Visual Basic for Applications Script
.vsmacros	Visual Studio .NET Binary-based Macro Project (Microsoft)
.vss	Visio Stencil (Microsoft)
.vst	Visio Template (Microsoft)
.vsw	Visio Workspace File (Microsoft)
.ws	Windows Script File

.wsc	Windows Script Component
.wsf	Windows Script File
.wsh	Windows Script Host Settings File

Screen Reference

Encryption Settings

Encryption



Emai Encryption Options

☐ Set message encryption default to on
☑ Attempt to decrypt inbound messages automatically
☐ Encrypt all outbound attachments

Default Encryption Method

○ Zip 2.0 encryption (weak)
● 128 Bit AES encryption standard
○ 256 Bit AES encryption standard
○ MessageLock 256-Bit AES encryption

Database: C:\Documents and Settings\Owner.ENCRYPTOMATIC-2\Application Data\MessageLock\Owner.mdb
Build: 216

This screen allows you to configure MessageLock default encryption behaviors.

Set message encryption default to on
This setting will always activate the email encryption button in the email toolbar. If you attempt to send to an email address that is not associated with a password, MessageLock will prompt you for the password and remember it the next time you send to that email address. You can always "deactivate" the tool button by clicking on it.

Attempt to decrypt inbound messages automatically
When MessageLock receives an encrypted message from another MessageLock system, it will try to decrypt the message automatically. If this setting is off, the message can be accessed at a later time by using the Zip Viewer.

Default Encryption Method
This is the encryption method that MessageLock will default to when you enter in a new recipient email address and password. on the "Manage Passwords Screen." 256-bit encryption is the strongest. We recommend using at least AES-128 bit encryption. Zip 2.0 (weak) encryption is included for the broadest compatibilty, but we do not recommend it.

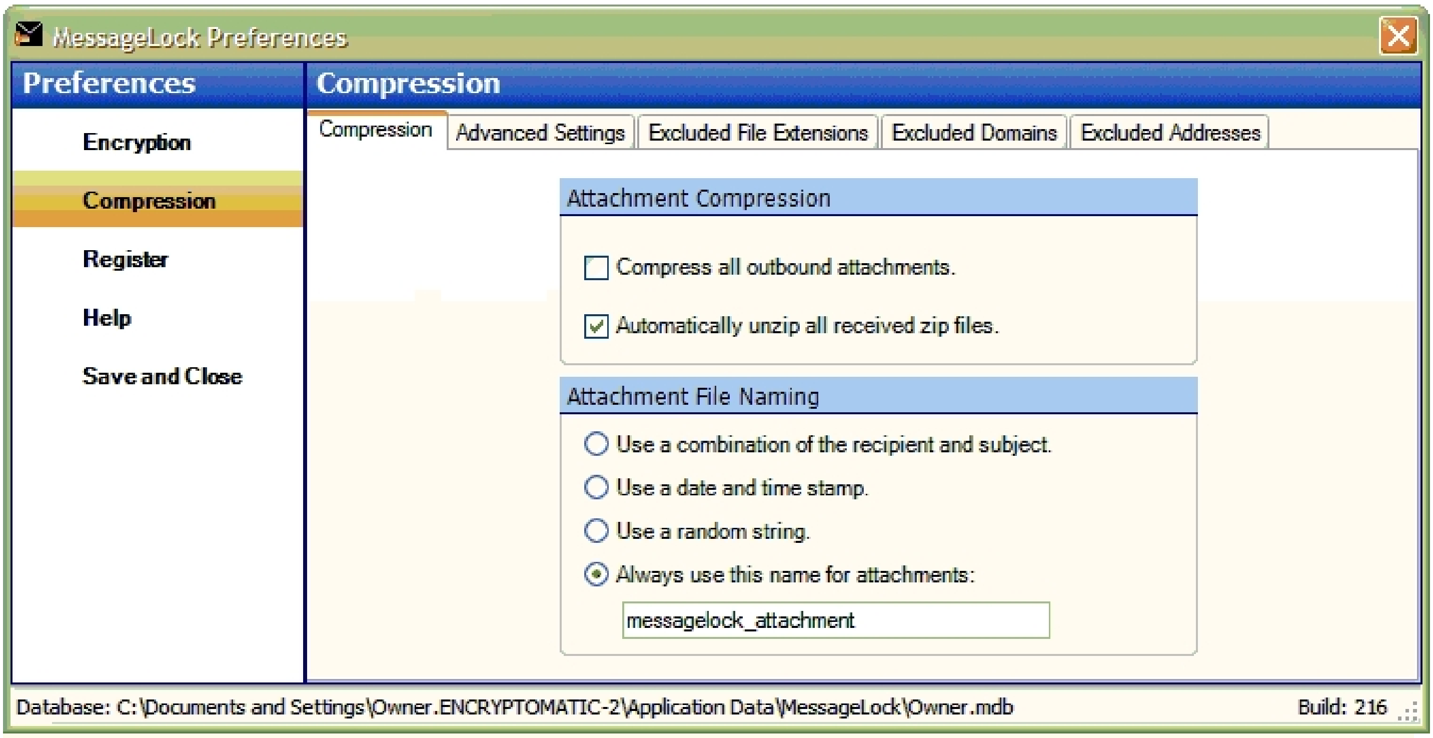
MessageLock AES-256 works well when the recipient is also using MessageLock, or if they have a special decryption tool.

For broadest compatiblity, we recommend using AES-128 bit zip compatible encryption.

Compression

Compression

The Compression tab allows you to configure how MessageLock handles file compression.



Attachment Compression

☐ Compress all outbound attachments.

☑ Automatically unzip all received zip files.

Attachment File Naming

○ Use a combination of the recipient and subject.

○ Use a date and time stamp.

○ Use a random string.

● Always use this name for attachments:

messagelock_attachment

Database: C:\Documents and Settings\Owner.ENCRYPTOMATIC-2\Application Data\MessageLock\Owner.mdb Build: 216

Compress all outbound attachments

This setting activates the Compress Files button on the email toolbar by default. This feature can be turned off by clicking the email toolbar.

Automatically unzip all received zip files

MessageLock will attempt to unzip all inbound email attachments that are in the .zip format. Although this feature is very convenient, you need to be aware of some dangers and shortcomings to using it.

Anti-Virus considerations

In our tests with a sampling of various anti-virus products, MessageLock did not interfere with the anti-virus' functions. In instances where viruses were detected, MessageLock was denied access by the anti-virus software to save the file to the email (which is the desired and correct behavior). However, we have not tested MessageLock with all anti-virus products, and we can not warrant that MessageLock will not interfere with all anti-virus software.

Outlook Security

If MessageLock unzips a file that violates Microsoft Outlook security (i/e the archive contains an executable file), Outlook may deny access to that file.

Because your data is so important, we have made the decision not to automatically delete the zip file after it is unzipped. This allows you to save any important files to your Windows Desktop for access. The downside is that more space is used in your Outlook inbox.

Attachment File Naming

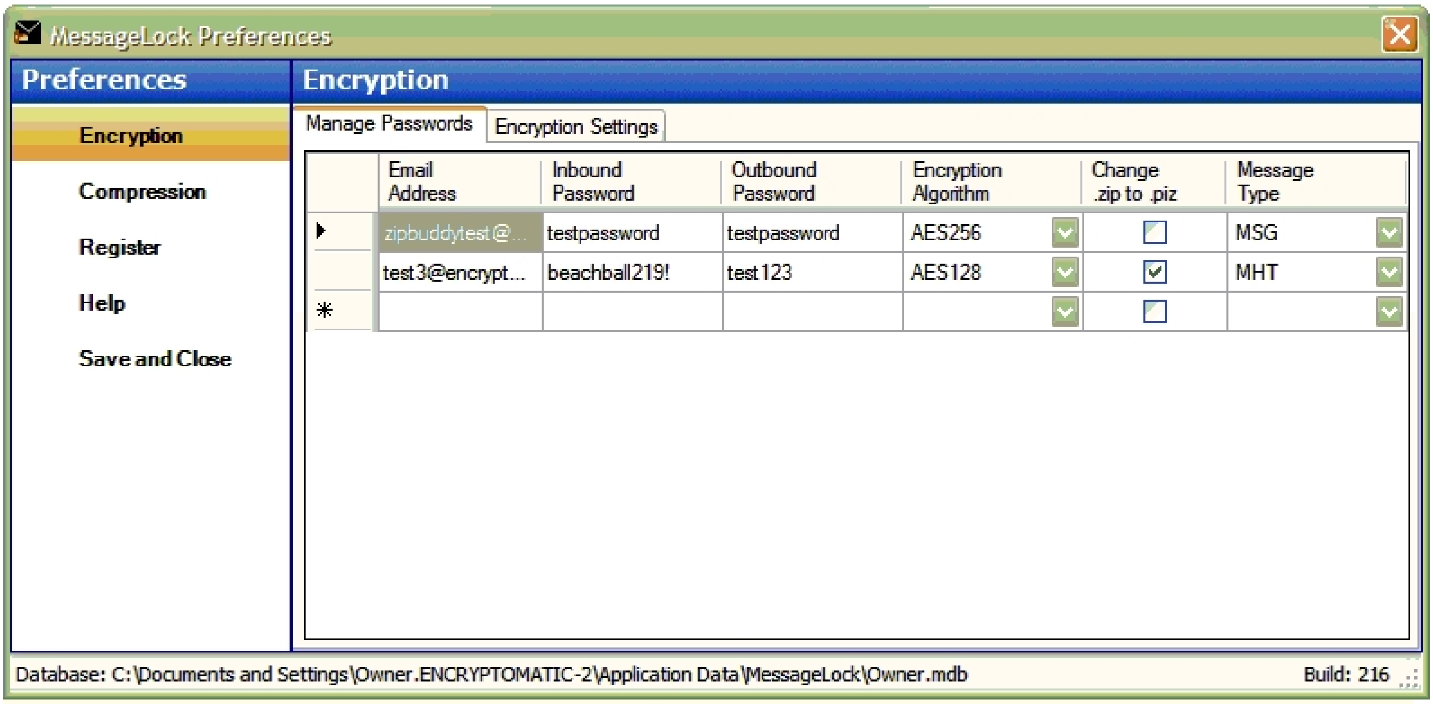
These options tell MessageLock how to name the attachments that it sends in your email. You can generate a unique name a number of ways, of you can simply always use a certain name.

Manage Passwords

Manage Passwords

The Manage Passwords Screen is where email addresses are associated with passwords.
When you send an email address and press the Encrypt button on the email toolbar, MessageLock searches this list for the "outbound" password.

When an encrypted file or message is received, MessageLock searches this list for the correct "inbound" password and uses it to attempt decryption.



	Email Address	Inbound Password	Outbound Password	Encryption Algorithm	Change .zip to .piz	Message Type
▶	zipbuddytest@...	testpassword	testpassword	AES256	☐	MSG
	test3@encrypt...	beachball219!	test123	AES128	☑	MHT
*					☐	

Database: C:\Documents and Settings\Owner.ENCRYPTOMATIC-2\Application Data\MessageLock\Owner.mdb Build: 216

You can select the preferred encryption method from a drop down list that appears when you click on the Encryption Method box.

To delete an email address

Click on the blue block directly in front of the email address you wish to delete. The row will be highlighted. Then press your Delete key.

To change any information in a row

Click on the information you wish to change, and retype.

Encryption Algorithm

The preferred level of encryption can be set for a specific email address. It can be changed at any time by clicking the down arrow and selecting the desired encryption.

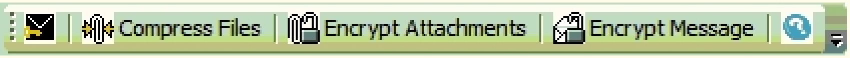
Change .zip to .piz

If you experience difficulty sending an encrypted .zip file to someone, it may be due to a very strict firewall policy setting that restricts .zip files in emails. Although most companies and ISPs allow .zip file attachments in email, some have aggressively restricted this common practice as a security precaution. If your recipient is subjected to such a restriction, you can tell MessageLock to always rename the .zip file to a .piz file. In most cases, the .piz file will arrive in the recipients inbox. However, the recipient will need to know how to save the .piz file as a .zip file so they can access it using a zip utility. A

Email Toolbar

Email Toolbar

When you click on Outlook's New Email button, Outlook opens a blank message. Notice that MessageLock places its toolbar with the Outlook tools (see below).



If a MessageLock toolbar item is highlighted (i/e orange), that indicates that feature has been selected for this message. Items may be highlighted because you clicked on them, or because you have set that as a default (See and Screen Reference for details on how to set defaults).

To select (or highlight) a MessageLock button, click on it.
To deselect (remove highlight) a button, click on it again.

Compress Files

If only the Compress Files button is highlighted, any attachment(s) to the email to be compressed into a zip file, and sent as an attachment. Compressing files can help save space and bandwidth, and is some times more convenient when sending many files.

Encrypt Attachments

This button will cause the attachments in a zip file to be encrypted. The receiver will need to have the password, and a zip utility (such as TugZip or Winzip 9.0 or 10.0) capable of decryption. If the recipient is also using MessageLock and has associated a password with your email address, the attachments can be decrypted automatically.

Note that Encrypt Attachments presently requires compression to be on.

Encrypt Message

Clicking on Encrypt Message will highlight all three buttons. When you encrypt the message, the text in the message as well as any file attachments will be encrypted and compressed into a zip file.

If your recipient also has MessageLock configured for your email address, the message and attachments can be automatically decrypted and restored. The receiver will know that the message was sent securely because MessageLock will append a short message to the bottom of the email noting the time and date that the message was processed.

If your recipient does not have MessageLock, they will need a zip utility (such as TugZip, IZarc, or WinZip 9.0 or later) capable of decrypting the file in the zip archive, and Microsoft Outlook.

MessageLock Settings

Click the email and key icon to access MessageLock's settings.

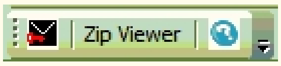
Help

Click the blue question mark button to see MessageLock's help file.

Attachment Viewer

Zip Viewer (aka Attachment Viewer)

If you open a message that contains a zip file, you will notice that a new option appears in the email toolbar, called the Zip Viewer.



Zip viewer lets you to view the files inside the zip attachment. If the files are encrypted, the viewer will use the MessageLock password file to attempt to decrypt the files.

The viewer will allow you to unzip (and decrypt if necessary) files directly into the email, or you can save the attachments to another location, such as your desktop.

We chose to use implement this Viewer in MessageLock for your convenience. The viewer links your encrypted zip files to the password archive. This approach allows you to continue using your default zip utility (such as TugZip, IZArc, or WinZip) as the default zip file processor by simply clicking on the zip file.

For more information on how the Item Viewer handles Outlook restricted file attachments, click here.

Registration Info

How to Purchase

How to Purchase

Thank you for your interest in purchasing a MessageLock license.

For information on registration please follow this link, www.encryptomatic.com

Email us with any questions that you have about licensing MessageLock or purchasing a site license to sales@encryptomatic.com, or call +1-218-287-5188

Support and Vendor Info

About Encryptomatic llc

About Encryptomatic llc

Our Mission:

To provide solutions that make our customers' lives more enjoyable and secure.

Our Vision

A safe world with the freedom to communicate freely and securely.

About Us

Encryptomatic llc is a privately held limited liability company headquartered in the historic downtown district of the twin towns of Moorhead, MN, and Fargo, ND USA, in heart of the beautiful Red River Valley of the North, where we enjoy snowy winters, beautiful summers, clean air, great fishing and an abundance of seasonal outdoor activities. Our average workday commute is about ten minutes.

We were founded in 2005 by our President, Darren Leno, a former Product Manager for Microsoft Business Solutions, and Great Plains Software, Inc.

For more information, please visit http://www.encryptomatic.com/about-us/

Technical Support

Technical Support

Online support for MessageLock, including a user forum, is available on our website: www.encryptomatic.com

A Frequently Asked Questions (FAQ) list is also available within this help file. The most up-to- date FAQ is posted on our website.

We invite you to use the comment form on our website to submit bug reports, feature requests, and usability comments. All submitted comments are reviewed by the product manager and given serious consideration.

Because Encryptomatic MessageLock was built for ease of use, and priced inexpensively, we can only attempt to provide a low level email support for clients who have not purchased an annual maintenance and support (M&S) contract. For information on purchasing a M&S contract, email us at support@encryptomatic.com.

FAQ

FAQ

I installed MessageLock, but I don't see it in Outlook. Where is it?

Open Outlook. You should see the MessageLock logo on the main Outlook toolbar. If that doesn't work, read on.

Can I only send encrypted messages and attachments to other MessageLock users?

Although MessageLock simplifies and streamlines the entire process of sending and receiving secured email, using the Zip format brings near universal Windows PC compatibility to MessageLock created messages. Anyone who has a zip utility installed on their computer and who knows the password should be able to open your message.

If someone you are sending an encrypted email message to doesn't want to install MessageLock, you can a) send to them using Zip 2.0 weak encryption, or b) ask them to consider installing Tugzip.

Using weak Zip 2.0 encryption provides the widest compatibility. Stronger compression, such as AES 128 or 256, requires a zip utility that incorporates AES standards. While more and more zip utilities are incorporating AES into their applications, not all of them have done so. A free zip utility that you may consider is TugZip. TugZip incorporates AES 256 encryption, and it has proven to work well in our lab with MessageLock. Other utilities that work well include WinZip and PKzip.

Does the recipient of my email need to use Outlook?

If the recipient has Outlook, they will find it convenient to receive your messages in .MSG Outlook file format.

For non-Outlook users, simply set the message format to .MHT. You can do this by accessing MessageLock preferences, locating the email address for this person, and changing the message format to .mht format. The recipient will now be able to view your message using their web browser.

How do I send an encrypted email to multiple recipients?

When sending an encrypted email message to multiple recipients, MessageLock will prompt you for a single-use "Group Password." Simply address the email message to multiple recipients, press "Encrypt Email" and MessageLock will prompt you for the group password.

I installed MessageLock. I see it listed in Window's Add/Remove Programs window, but it does not appear in Outlook's File menu. What's going on?

On Windows XP, MessageLock requires that the .Net Framework version 2 reside on your PC. Although this usually installs automatically at the time you run the MessageLock installer, in some cases the framework needs to be installed independently. First, go to Control Panel>Add/Remove Programs and see if Microsoft .Net Framework 2 is installed on your PC.

If .Net Framework 2 is installed, you should uninstall MessageLock from Add/Remove programs, reboot your PC, and install it again. Be sure that Outlook is not running when you install MessageLock.

What's an inbound password?

This is the password that a sender will use to encrypt a file he is sending you. Your friend's outbound password is your inbound password.

What's an outbound password?

This is the password that you will use to encrypt a file you are sending to someone. Your outbound password is someone else's inbound password.

When MessageLock automatically decompresses and decrypts my inbound email attachments, it leaves the zip file in the message. Why doesn't it delete the file?

Encryptomatic LLC takes your data very seriously. Our user testing showed that some people wanted the zip file to be removed, while others had legitimate reasons for wanting to preserve the zip file. We decided that deleting any data on your computer is very serious business, and must be your decision. We may revisit this issue in a subsequent version after we gather additional feedback for requirements, perhaps as a user definable rule. If you would like us to consider your input, email us at support at Encrytomatic.com.

Are MessageLock zip files compatible with other Zip utilities?

Yes, zip files created by MessageLock can be read by virtually any other zip program.

Can I use WinZip or PKzip to view and decrypt MessageLock attachments?

Yes, you can use virtually any unzip program to open a .zip file created and encrypted by MessageLock. If you encrypt with the less secure Zip2.0 algorithm, you will have more compatibility but less security. We recommend using an unzip program that supports AES256 encryption and utilizing strong encryption.

Will MessageLock replace my default or system Zip utility?

No. Your default zip utility is unaffected.

When I double click a zip file in an Outlook message, my default Zip utility opens it. Why doesn't MessageLock open the file?

MessageLock does not want to be your default zip utility. If you want to view, decompress or decrypt a zip file in an Outlook, just open the email message by double clicking on it, then click on the Viewer button from the MessageLock toolbar.

Which encryption algorithms do you support?

MessageLock provides support for the classic Zip2.0 encryption, AES128, and AES256. Zip2.0 is the least secure, but provides the most compatibility with older unzip programs. AES256 is the newest and most secure, and is being incorporated into newer versions of unzip programs, such as WinZip and PKZip.

MessageLock also provides "MessageLockAes256". This is a more secure implementation of the AES256 algorithm, because it encrypts the entire zip file rather than just the individual files within the Zip archive. This approach prevents snoops from culling information from the names of the documents inside the zip archive. By protecting file names, MessageLockAES256 provides no clues as to the significance of the data. This algorithm is best used between users of MessageLock.

How do I remove MessageLock from my PC?

Go to your Control Panel, and select Add/Remove programs. Scroll to the bottom of your list, and look for MessageLock. Click on it and select Uninstall.

Do you offer telephone or email support?

We attempt to answer email requests, usually within 48 hours. Users who do not have a maintenance and support contract with us receive low priority support. We offer phone and high priority email support only for corporate users who purchase an annual support agreement. On-site user training and consulting is available. Please contact us at support@encryptomatic.com for more information.

MessageLock is still appearing in my Outlook Tools menu after it was uninstalled, or MessageLock appears in the Tools menu more than once.

Simply reset the tools menu. Select Tools>Customize, click on "Menu Bar" to highlight, and then select the Reset button. Exit Outlook and then restart it.

Does MessageLock Protect all of the data on my PC?

No. MessageLock only protects your email as it travels from your PC to your intended recipient's PC. Although this is a very important piece of the overall puzzle in securing your data, you need to know that in the following circumstances, MessageLock may not provide protection for your communications and data.

* if you use weak passwords.
* if you share your passwords with others, or if your password is intercepted as you share it.
* if multiple people use your PC and have access to your files.
* MessageLock does not encrypt data on your hard drive (visit our store for products that will).
* you passwords could be stolen by key loggers, trojan horses or viruses (visit our store for products that can combat these threats).
* you should use password protection within Outlook and Microsoft Windows to protect access to your PC.

* if you fail to properly configure and implement a firewall to protect your computer from attacks from hackers.
* the recipient can forward and share your message after it is received.
* if you share access to your Outlook files purposefully or accidentally to users of a WAN or LAN.
* if the recipient does not take adequate protections, your communications may be vulnerable on the recipient's PC.
* Other threats, known or unknown, may exist or someday be developed.

How do I submit a bug report?

We appreciate your reports. Send your report to support@encryptomatic.com, or enter them in our form on www.encryptomatic.com. Be sure to include the version of Outlook you are running, your operating system and name/model of your PC. We track and review all bug reports.

I love MessageLock! But I have ideas that could make it even better!

We appreciate that you want to help us improve MessageLock, and we relish your ideas. Send them to Support@Encryptomatic.com.

I lost my Product Key. How can I get it replaced?

Send an email to support@encryptomatic.com from the email address that you used to register MessageLock. We will respond with your key.

Why does MessageLock use zip compression and AES encryption to protect my email and attachments?

Most people understand the need to secure their communications, but they do nothing about it because it is simply too difficult to implement. MessageLock seeks to remove the complexity and allow anyone to easily, seamlessly protect their email communications. We believe that the zip AES256 encryption provides a safe, practical and universal method of protection. Even if a receiver doesn't have MessageLock, they can still access the encrypted data if they have the password and one of many unzip programs that supports AES256. Of course we hope everyone will use MessageLock because of the convenience it provides at an low price.

Is MessageLock Hipaa Compliant?

Hipaa compliance is a U.S. government mandate requiring organizations to take steps to protect access to sensitive information in order to protect personal privacy. MessageLock's AES-128 and 256-bit encryption exceeds Hippa's encryption strength requirements. MessageLock may be an important component of your organization's overall effort to achieve compliance with Hippa regulations, but will not on its own make you compliant: full compliance requires that appropriate systems, checks and processes be in place across your organization.

Is a longer password more secure than a shorter password?

Yes, the longer the better. Of course, even a short password is better than not encrypting your data at all, but if you want the most protection then use a strong password. We recommend using the password Key Generator in MessageLock to produce the most secure passwords.

I want to: a) license your source code, b) interview your executives for a news article, c) invite you to keynote a tradeshow, e) buy your company, f) order a site license for more than 500 users, or g) want to sell you my company

Then we'd like to speak with you, too. Email us: support@encryptomatic.com