**Tools**

*These links are for your use only, as sources of images used below if they are not high quality enough in this doc.*

1. Adium tool guide [– Link](https://ssd.eff.org/en/module/how-use-otr-mac)
2. Basic Security Setup for Android - [Link](https://securityinabox.org/android_basic)
3. ChatSecure tool guide - [Link](https://ssd.eff.org/en/module/how-install-and-use-chatsecure)
4. Cobian Backup Guide - [Link](https://securityinabox.org/cobian_main)
5. How to change your Facebook privacy settings - [Link](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)
6. How to opt-out of Facebook's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)
7. How to opt-out of Twitter's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)
8. Jitsi Tool guide – [Link](https://securityinabox.org/jitsi)
9. K9 & APG tool guide – [Link](https://securityinabox.org/k9_apg_main)
10. KeePass tool guide – [Link](https://securityinabox.org/keepass_main)
11. ObscuraCamTool guide – [Link](https://securityinabox.org/obscuracam_main)
12. Orbot & Orweb tool guide – [Link](https://securityinabox.org/Orbot_main), [Link](https://securityinabox.org/orweb_main)
13. PGP for Linux tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-linux)
14. PGP for Mac O SX tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x)
15. PGP for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-windows-pc)
16. Pidgin tool guide – [Link](https://ssd.eff.org/en/module/how-use-otr-windows)
17. Psiphon3 tool guide – [Link](https://www.level-up.cc/leading-trainings/training-curriculum/deepening/psiphon3)
18. Recuva – File Recovery Guide – [Link](https://securityinabox.org/recuva_main)
19. Redphone Tool guide – [Link](https://ssd.eff.org/en/module/how-use-redphone-android)
20. Signal Tool guide – [Link](https://ssd.eff.org/en/module/how-use-signal-%E2%80%93-private-messenger)
21. TextSecure tool guide – [Link](https://ssd.eff.org/en/module/how-use-textsecure-android)
22. Tor for Mac tool guide – [Link](https://www.torproject.org/projects/torbrowser.html.en#macosx)
23. Tor for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/)
24. TrueCrypt Tool Guide – [Link](https://securityinabox.org/truecrypt_main)

**ADIUM TOOL GUIDE**

# Adium & OTR Tool Guide

# Secure instant messaging for Mac

**Lesson to read: Sending a Message**

**Download Location:** <https://adium.im/>

**Computer requirements** (Adium 1.5 or later): Mac OS X 10.6.8 or newer, an Apple-branded Macintosh computer.

**Version used in this guide:** Adium 1.5.9

**License:** GNU GPL

**Other reading:** <https://pressfreedomfoundation.org/encryption-works>;<https://adium.im/help/>

**Level:**Beginner-Intermediate

**Time required:** 15-20 minutes

## Adium is a free and open source instant messaging client for OS X that allows you to chat with individuals across multiple chat protocols, including Google Hangouts, Yahoo! Messenger, Facebook chat, Windows Live Messenger, AIM, ICQ, and XMPP.

## OTR (Off-the-record) is a protocol that allows people to have confidential conversations using the messaging tools they’re already familiar with. This should not be confused with Google's “Off the record,” which merely disables chat logging, and does not have encryption or verification capabilities. For Mac users, OTR comes built-in with the Adium client.

## OTR employs end-to-end encryption. This means that you can use it to have conversations over services like Google Hangouts or Facebook without those companies ever having access to the contents of the conversations. This is different from the way in which Google and AOL use the term “off the record” to mean that a conversation is not being logged; that option does not encrypt your conversation.

## Why should I use Adium + OTR?

## When you have a chat conversation using Google Hangouts or Facebook chat on the Google or Facebook websites, that chat is encrypted using HTTPS , which means the content of your chat is protected from hackers and other third parties while it’s in transit. It is not, however, protected from Google or Facebook, which have the keys to your conversations and can hand them over to authorities.

## After you have installed Adium, you can sign in to it using multiple accounts at the same time. For example, you could use Google Hangouts, Facebook, and XMPP simultaneously. Adium also allows you to chat using these tools without OTR. Since OTR only works if both people are using it, this means that even if the other person does not have it installed, you can still chat with them using Adium.

## Adium also allows you to do out-of-band verification to make sure that you’re talking to the person you think you’re talking to and you are not being subject to a MITM attack. For every conversation, there is an option that will show you the key fingerprints it has for you and the person with whom you are chatting. A "key fingerprint" is a string of characters like "342e 2309 bd20 0912 ff10 6c63 2192 1928,” that’s used to verify a longer public key. Exchange your fingerprints through another communications channel, such as Twitter DM or email, to make sure that no one is interfering with your conversation.

## Limitations: When should I not use Adium + OTR?

## Technologists have a term to describe when a program or technology might be vulnerable to external attack: they say it has a large “attack surface.” Adium has a large attack surface. It is a complex program, which has not been written with security as a top priority. It almost certainly has bugs, some of which might be used by governments or even big companies to break into computers that are using it. Using Adium to encrypt your conversations is a great defense against the kind of untargeted dragnet surveillance that is used to spy on everyone's Internet conversations, but if you think you will be personally targeted by a well-resourced attacker (like a nation-state), you should consider stronger precautions, such as PGP -encrypted email.

## Installing Adium + OTR On Your Mac

### Step 1: Install the program

First, go to <https://adium.im/> in your browser. Choose “Download Adium 1.5.9.” The file will download as a .dmg, or disk image, and will probably be saved to your “downloads” folder.

Double-click on the file; that will open up a window that looks like this:

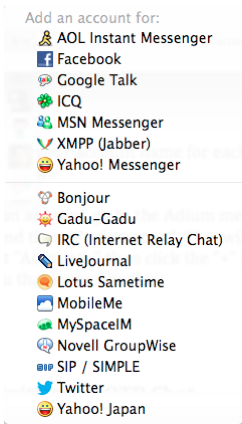


Move the Adium icon into the “Applications” folder to install the program. Once the program is installed, look for it in your Applications folder and double-click to open it.

### Step 2: Set up your account(s)

First, you will need to decide what chat tools or protocols you want to use with Adium. The setup process is similar, but not identical, for each type of tool. You will need to know your account name for each tool or protocol, as well as your password for each account.

To set up an account, go to the Adium menu at the top of your screen and click “Adium” and then “Preferences.” This will open a window with another menu at the top. Select “Accounts,” then click the “+” sign at the bottom of the window. You will see a menu that looks like this:



Select the program that you wish to sign in to. From here, you will be prompted either to enter your username and password, or to use Adium’s authorization tool to sign in to your account. Follow Adium’s instructions carefully.

## How to Initiate an OTR Chat

Once you have signed in to one or more of your accounts, you can start using OTR.

Remember: In order to have a conversation using OTR, both people need to be using a chat program that supports OTR.

### Step 1: Initiate an OTR chat

First, identify someone who is using OTR, and initiate a conversation with them in Adium by double-clicking on their name. Once you have opened the chat window, you will see a small, open lock in the upper left-hand corner of the chat window. Click on the lock and select “Initiate Encrypted OTR Chat.”

### Step 2: Verify your connection

Once you have initiated the chat and the other person has accepted the invitation, you will see the lock icon close; this is how you know that your chat is now encrypted (congratulations!) – But wait, there’s still another step!

At this time, you have initiated an unverified, encrypted chat. This means that while your communications are encrypted, you have not yet determined and verified the identity of the person you are chatting with. Unless you are in the same room and can see each other’s screens, it is important that you verify each other’s identities. (For more information, read the EFF module on [Key Verification](https://ssd.eff.org/en/module/key-verification" \l "overlay=en/node/37/" \t "_blank).)

To verify another user’s identity using Adium, click again on the lock, and select “Verify.” You will be shown a window that displays both your key and the key of the other user. Some versions of Adium only support manual fingerprint verification. This means that, using some method, you and the person with whom you’re chatting will need to check to make sure that the keys that you are being shown by Adium match precisely.

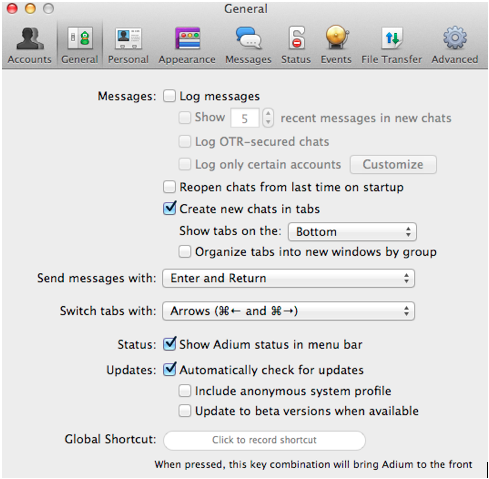
The easiest way to do this is to read them aloud to one another in person, but that’s not always possible. There are different ways to accomplish this with varying degrees of trustworthiness. For example, you can read your keys aloud to one another on the phone if you recognize each other’s voices or send them using another verified method of communication such as PGP. Some people publicise their key on their website, Twitter account, or business card.

The most important thing is that you verify that every single letter and digit matches perfectly.

### Step 3: Disable logging

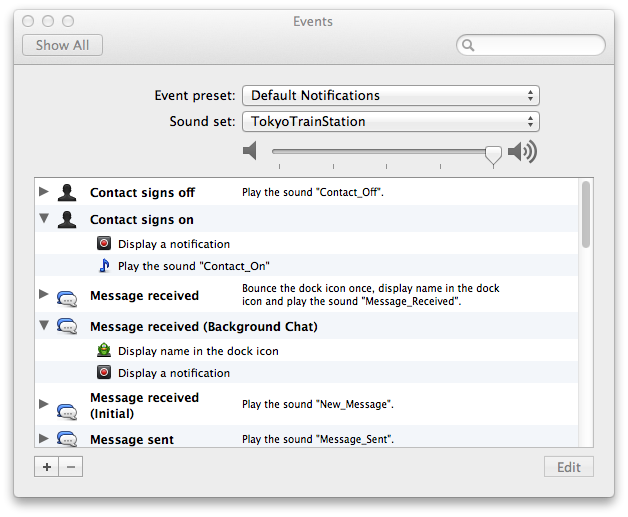
Now that you have initiated an encrypted chat and verified your chat partner’s identity, there’s one more thing you need to do. Unfortunately, Adium logs your OTR-encrypted chats by default, saving them to your hard drive. This means that, despite the fact that they’re encrypted, they are being saved in plain text on your hard drive.

To disable logging, click “Adium” in the menu at the top of your screen, then “Preferences.” In the new window, select “General” and then disable “Log messages” and “Log OTR-secured chats.” Your settings should now look like this:



Also, when Adium displays notifications of new messages, the contents of those messages may be logged by the OS X Notification Center. This means that while Adium leaves no trace of your communications on your own computer or your correspondent's, either your or their computer's version of OS X may preserve a record. To prevent this, you may want to disable notifications.

To do this, select "Events" in the Preferences window, and look for any entries that say "Display a notification." For each entry, expand it by clicking the gray triangle, and then click the newly-exposed line that say "Display a notification," then click the minus icon ("-") at the lower left to remove that line." If you are worried about records left on your computer, you should also turn on full-disk encryption, which will help protect this data from being obtained by a third party without your password.



**BASIC SECURITY SETUP FOR ANDROID GUIDE**

# Basic Security Setup for Android guide

**Lesson to read: Mobile Phones**

**Phone requirements:** Android 4.4

**Level:**Beginner

**Time required:** 5 minutes

## 1.0 Basic Setup

## 1.1 Access to your phone

**Enable** Lock SIM card, found under Settings -> Personal -> Security -> Set up SIM card lock. This will mean that you must enter a PIN number in order to unlock your SIM card each time your phone is switched on, with out the PIN no phone calls can be made.

**Set up** a Screen Lock, found under Settings -> Personal -> Security -> Screen Lock, which will ensure that a code, pattern or password needs to be entered in order to unlock the screen once it has been locked. We recommended using the PIN or Password option, as these are not restricted by length. You can find more information on creating strong passwords in the Passwords lesson.

**Set** the security lock timer, which will automatically lock your phone after a specified time. You can specify a value which suits you, depending on how regularly you are willing to have to unlock your phone.

## 1.2 Device Encryption

If your device uses Android version 4.0 or newer, you should **turn on** device encryption. This can be done in Settings -> Personal -> Security -> Encryption. Before you can utilise device encryption, however, you will be required to set a screen lock password (described above).

**Note:** Before starting the encryption process, ensure the phone is fully charged and plugged into a power source.

## 1.3 Network settings

**Turn off** Wi-Fi and Bluetooth by default. Ensure that Tethering and Portable Hotspots, under Wireless and Network Settings, are switched off when not in use. Settings -> Wireless & Networks -> More -> Tethering & Mobile hotspot

If your device supports Near Field Communication (NFC), this will be switched on by default, and so must be switched off manually.

## 1.4 Location settings

**Switch off** Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings -> Personal -> Location).

**Note**: Only turn on location settings as you need them. It is important not have these services running by default in the background as it reduces the risk of location tracking, saves battery power and reduces unwanted data streams initiated by applications running in the background or remotely by your mobile carrier.

## 1.5 Caller Identity

If you want to hide your caller-ID, go to Phone Dialler -> settings -> Additional Settings -> Caller ID -> hide number.

## 1.6 Software Updates

To ensure that you phone remains secure it is strongly recommended to keep your software updated. There are two types of updates that need to be checked

The phone operating system: go to: settings -> About phone -> updates -> check for updates

Apps you have installed: Open the **Play store** app, from the side menu select **My Apps**.

**Note:** When updating your phones software it is important to do it from a trusted location such as your internet connection at home instead of somewhere like an internet cafe or coffee shop.

**CHATSECURE TOOL GUIDE**

# ChatSecure Tool Guide

# Secure texting for iPhone and Android

**Lesson to read: Sending a Message**

**Download location:**[https://chatsecure.org](https://chatsecure.org/); can also be downloaded from the [Apple App store](https://itunes.apple.com/us/app/chatsecure/id464200063" \t "_blank) or the [Google Play store](https://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im" \t "_blank).

**System requirements:**iOS 6.0, Android (varies)

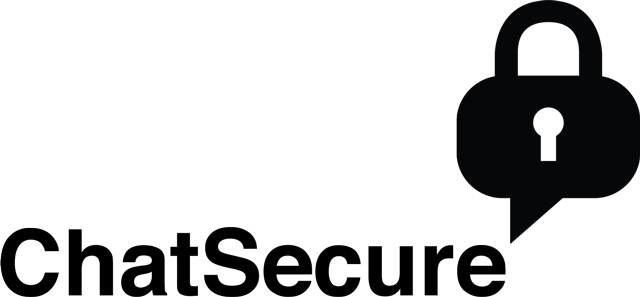
**Version used in this guide:**2.2.4 (iPhone), 13.1.2 (Android)

**License:**Apple, GPLv3; Android, Apache 2.0

**Other reading:**<https://guardianproject.info/apps/chatsecure/>

**Level:**Beginner-Intermediate

**Time required:**5-10 minutes



ChatSecure is a free mobile phone application for iPhone and Android devices that allows users to communicate with off the record instant messaging. ChatSecure allows users to send instant messages and chats using a cell phone, instead of with a traditional desktop or laptop computer. It's compatible with iPhone and Android phones.

ChatSecure supports OTR encryption over XMPP. All messages sent via ChatSecure are completely private, so long as the person you are chatting with is also using an OTR compatible instant messaging client like ChatSecure, Adium, Pidgin, or Jitsi. The app’s capabilities allow it to deliver audio messages, photos, files, or text.

When you send messages using ChatSecure, they are not stored on the phone system's memory. ChatSecure used with the privacy plugin Orbot should be able to bypass most firewalls, network restrictions, and blacklists. The app can manage multiple accounts, so you can chat with your Facebook friends, Google contacts, or other privacy conscious users that use an instant messaging program that supports OTR encryption.

**How to install and configure ChatSecure**

1. Download and install ChatSecure

Visit the Apple App Store or Google Play store and search for ChatSecure by The Guardian Project. Select “Install” and accept the Terms of Service by clicking “Accept.” The app will download and install automatically.

2. Open the app and set your password

When you open the app you will be promoted to set a password. You will be prompted to create a passphrase in order to locally encrypt your data. If you choose to do this, your data will be encrypted in transit, as well as encrypted locally on your phone.

If you choose to skip this step, your messages will still be encrypted in transit, but will not be protected on your device. For more information on selecting a strong passphrase, see the Passwords lesson.

3. Configure your accounts

You can add a variety of different accounts your ChatSecure app. To add GoogleTalk or Google Hangouts, choose “Google.” To add any XMPP or Jabber messaging service, choose “Jabber (XMPP).” To add your Facebook account, also choose “Jabber (XMPP).”

Once you’ve added your account, type in your username (or email address) and your password to sign in. Your contacts should load automatically.

To add a second or third account, click on the “accounts” tab in the menu. In the upper right hand corner, click on the “+” sign. You can either choose to add an existing account or create a new account.

**How to use ChatSecure**

1. Sign in to your accounts

To sign in to your account, click on the “accounts” tab in the menu and turn on the accounts you wish to use. Once you sign in, anyone can connect with you from a mobile or desktop instant messaging application.

2. Start end-to-end encryption

Once you’ve started a chat with someone, click on the unlocked lock icon on the top menu bar of the display. Choose “Start Encryption.” If the person you are chatting with has an OTR compatible instant messaging system, then you will have the option to verify your (and their) fingerprint.

ChatSecure offers three ways to verify OTR fingerprints, but if you're chatting with someone over a desktop instant messenger and not with ChatSecure, the best way to verify an OTR fingerprint is by communicating through another channel. You can resend your fingerprint over an SMS (TextSecure), say it over the phone if you recognize one another's voices, use PGP email, or verify in person. Click on “manual verification” and ChatSecure will display your and your friend's fingerprints. If you can confirm that you both have the same information, you can click “verify.”

ChatSecure supports manual verification or verification by scanning the other user’s barcode (QR). If you are in the same room as the other person, you can easily scan the barcode on their phone or read your keys aloud to one another.

3. Understand your options

* Just like a desktop instant messaging service, ChatSecure gives you the option to appear offline, busy, idle, or away. To change this setting click on your name at the top of your friends list.
* ChatSecure also allows you to initiate group chats and add new contacts, both of which can be done from the main menu. (Note that group chats *cannot be secured* like one-on-one chats due to limitations of the OTR protocol.)
* The app supports multimedia messaging, can take pictures, and can send photos and files securely if your friend is also using end-to-end encryption and you are able to verify her identity.
* ChatSecure gives you the option to create a new XMPP or Jabber messaging account that supports OTR encryption. If you don't already use XMPP messaging, this is a great opportunity to create one and experiment with non-proprietary messaging.

**COBIAN BACKUP TOOL GUIDE**

# Cobian Backup

# Backing up your computer files

**Lesson to read: Backing Up**

**Download Location:** [**http://www.cobiansoft.com/cobianbackup.htm**](http://www.cobiansoft.com/cobianbackup.htm)

**Computer requirements:**

* XP, 2003, Vista, 2008, Windows 7
* Windows 95, 98 and ME are compatible with Cobian version 7.

**Version used in this guide:** Cobian 10

**License:** Freeware

**Level:** Intermediate

**Time required:** 30 minutes

* 1. **Things you should know about this tool before you start**

Cobian Backup is used to archive, (or to make a backup copy) of your files and directories. Backups can be stored in other directories or drives on your computer, other computers on the office network, or on removable devices (CDs, DVDs and USB memory sticks). Cobian Backup lets you archive your directories and files on a regular basis. It works silently in the background on your system (that is, in the system tray), checking your schedule and executing the backup process when necessary. Cobian Backup can also compress and encrypt files as it generates the backup file.

Using Cobian will give you:

* The ability to back up all documents, files and folders
* The ability to compress and decompress your backup files
* The ability to encrypt and decrypt your archived files

**Installing Cobian – in brief**

* Open www.cobiansoft.com/cobianbackup.htm
* Click on the link "Download Cobian Backup" on the page.
* Save the installer, then find it and doubleclick it
* Read the 'Installation Note' below before you continue
* After you have successfully installed Cobian you may delete the installation program from your computer.

## 2.0 How to Install Cobian Backup

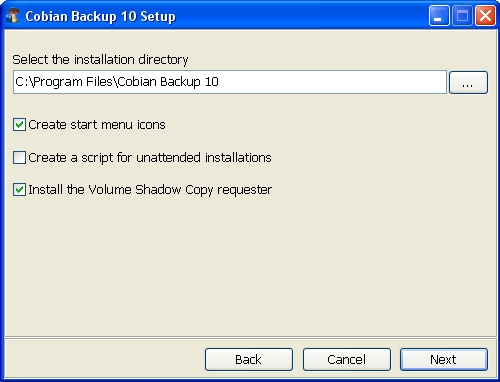
**Installation Note**: Before you begin the installation process, verify that you have both the latest versions of the **Microsoft Windows Installer** and the **Microsoft.NET Framework**.

Installing **Cobian Backup**is a relatively easy and quick procedure.

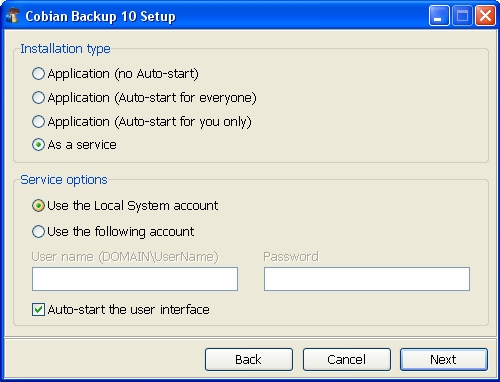
**Step 1**. **Double click “**cbsetup.exe”; the Open File - Security Warning dialog box may appear. If it does, **click “**Run” to activate the light blue Extracting the resource progress status bar, followed a few moments later by the following screen:



**Step 2**. Click “Next” to activate the *Please read and accept the license agreement* screen; check the *I accept* option, and then click “Next” again to activate the following screen:

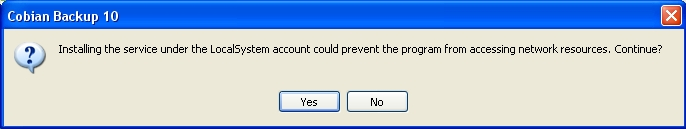


**Step 3**. Click “Next” to activate the following screen:



**Step 4**. Check the *Use Local System account* option in the *Service options* pane, so that your own resembles *Figure 3* above. This option ensures that Cobian Backup will be running silently in the background all the time, so that your backups will occur as scheduled.

**Step 5**. Click “Next” to activate the following message prompt:



**Step 6**. Click “Yes” to activate the next installation screen, and then click “Next” to continue with the installation process.

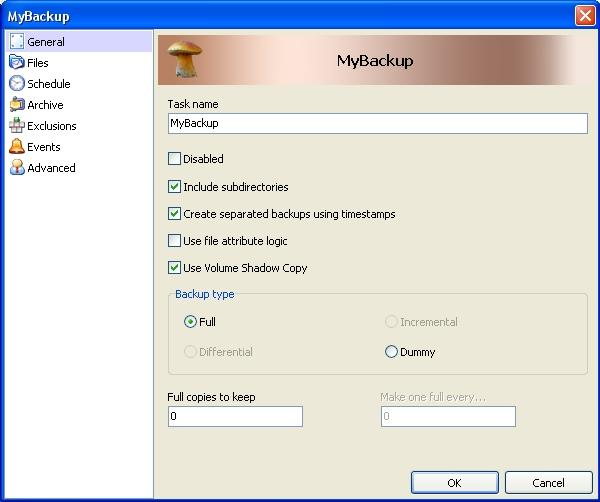
**Step 7**. Click “Done” to complete the installation process. After the installation process has been completed, the Cobian Backup icon will appear in the **Windows System Tray**.

**2.1 How to Backup Your Directories and Files**

In this section you will learn how to perform a simple backup or archive of a specified files and/or folders. Cobian Backup uses a *backup task* which can be configured to include a specified group of files and/or folders. A backup task can be set to run on a specified day and time.

To create a new backup task, perform the following step:

**Step 1**. Click “Schedule” to create a new backup task, and activate the *New task* window as follows:



The left sidebar lists a number of tabs and their associated screens - used to set different backup options and parameters - are displayed in the pane at right. All the options in the *General* tab are described below:

**2.1.1 Option Descriptions**

*Task Name*: This *Task Name* text field lets you enter a name for the backup task. Use a name that identifies the nature of the backup. For example, if the backup is going to contain video files, you could name it *Video Backup*.

*Disabled*: This option *must* be left unchecked.

Warning: Enabling the *Disabled* option will override the rest of the options, and prevent the backup task from running.

*Include Subdirectories*: This option lets you include all the subdirectories/folders within a selected directory/folder for the backup task. This is an efficient method for backing up a large number of folders and/or files. As an example, if you select the*My Documents* folder and check this option, then all files and folders in *My Documents* will be included in the backup task.

*Create separated backups using timestamps*: This option lets you specify that the date and time of the backup task will be automatically included in the folder name containing your backup file. This is a good idea because it means that you will easily be able to identify when the backup was performed.

*Use file attribute logic*: This option is only relevant when you choose to perform an incremental or differential backup (see below). File attributes contain information about the file.

**Note**: The following option is only available for Windows OS versions more recent than *and* including Windows XP.

*Use Volume Shadow Copy*: This option lets you backup files which are locked.

Cobian Backup verifies this information to determine whether there has been a change in the source file from the last time a backup was performed. If you then run an *Differential* or *Incremental* backup, the file will be updated.

**Note**: You will only be able to run a full or 'dummy backup' if you *disable this option* (the dummy backup option is explained below).

**2.1.2 Backup type Descriptions**

*Full*: This option means that *every* single file in the source location will be copied to your backup directory. If you have enabled the *Create separated backups using timestamp* option, you will have several copies of the same source (identified by the time and date of the backup in the folder title). Otherwise, Cobian Backup will overwrite the previous version (if any).

*Incremental*: This option means the program will verify if the files selected for backup have been changed since the last backup was performed. If there has been no change, it will be skipped over during the backup process, saving backup time. The *Use file attribute logic* option needs to be checked in order to perform this backup.

*Differential*: The program will check if the source has been changed from the last **full** backup. If there is no need to copy that file, it will be skipped, saving backup time. If you have run a full backup before on the same set of files, then you can continue backing it up, using the Differential method.

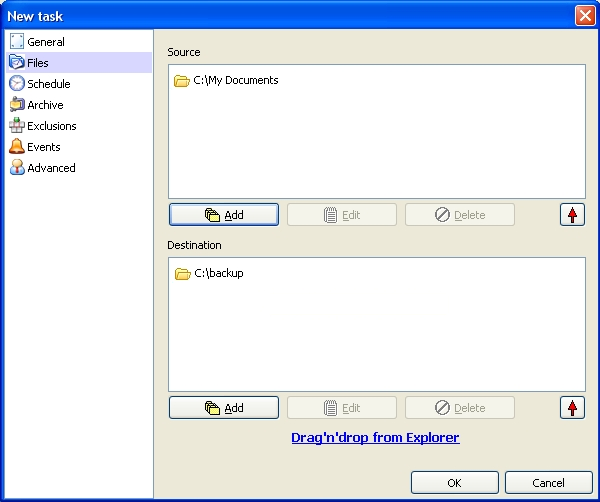
*Dummy task*: You can use this option to get your computer to run or shut down programs at certain times. This is a more advanced option which is not really relevant to our basic backup procedure.

**Step 2**. Click “OK” to confirm your search options and parameters for your backup task.

**2.2 How to Create a Backup File**

To begin creating a backup file, perform the following steps:

**Step 1**. Click “Files” in the left sidebar of the *New task* window to display a *blank* version of the following screen:



**Step 2**. Select the files you want to back up. (In *Figure 3* above, the *My Documents* folder is selected.)

**Step 3**. Click “Add” in the *Source* pane to activate the *Directory* menu.

**Step 4**. Select *Directory* if you want to back up an entire directory, and *Files* to back up individual files. To specify individual files or directories to be backed up, select *Manually*, and type in the file path or directory for your backup.

**Note**: You can add as many files or directories as you like. If you wish to back up files currently on your FTP server, choose the *FTP site* option (you will need to have the appropriate server login details).

When you have selected the files and/or folders, they will appear in the *Source* area. As you can see in *Figure 3* above, the *My Documents* folder is displayed there, meaning this folder will now be included in the backup task.

The *Destination* pane specifies where the backup will be stored.

**Step 5**. Click “Add” in the *Destination pane* to activate the Directory menu.

**Step 6**. Select *Directory* to open a browser window where you select the destination folder for your backup file.

**Note**: If you want to create several versions of the backup file, you may specify several folders here. If you selected the *Manually* option, you must type in the full path to the folder where you want to keep the backup. To use a remote Internet server to store your archive, select the *FTP site* option (you will need to have the appropriate server login details).

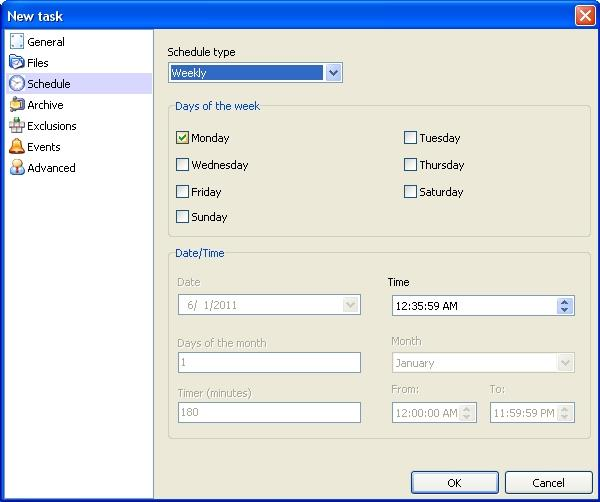
The screen should now resemble the example above example with file(s) and/or folder(s) in the source area and folder(s) in the destination area. However, don't click *OK* just yet! You still need to set a schedule for your backup.

**2.3 How to Schedule Your Backup Task**

For your automatic backup to work, you need to fill in the *Schedule* section. This section lets you specify when you want the backup to be performed.

To set the schedule options, perform the following steps:

**Step 1**. Select “Schedule” from the left sidebar, to activate the following pane:



The *Schedule type* options are listed in the drop-down menu, and described below:

*Once*: The backup will be done once only at the date and time specified in the *Date/Time* area.

*Daily*: The backup will be done every day at the time specified in the *Date/Time* area.

*Weekly*: The backup will be done on the days of the week selected. In the example above, the backup will be done on Fridays. You may select other days also. The backup will be done on all days selected at the time specified in the *Date/Time* area.

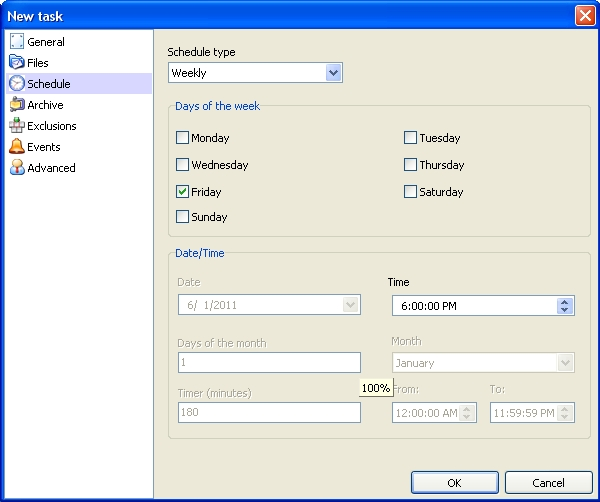
*Monthly*: The backup will be done on the days typed into the days of the month box at the time specified in the *Date/Time* area.

*Yearly*: The backup will be done on the days typed into the days of the month box, during the month specified, and at the time specified in the *Date/Time* area.

*Timer*: The backup will be done repeatedly at intervals specified in the Timer text box in the *Date/Time* area.

*Manually*: You will have to run the backup yourself from the main program window.

**Step 2**. Click “OK” to confirm the options and settings for the backup schedule as follows:

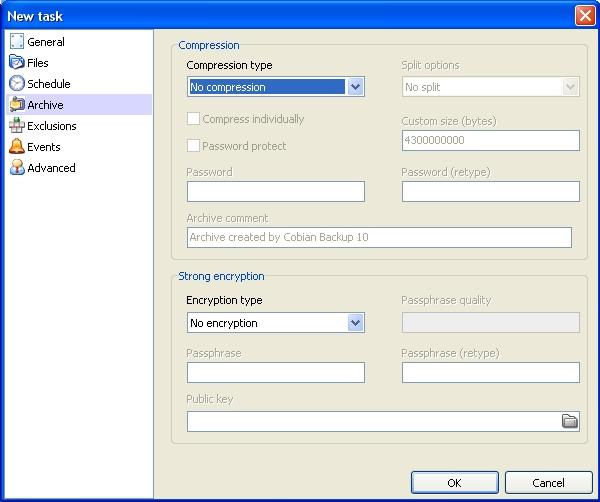


Once you have decided on a backup schedule, you have completed the final step. The backup will now run on the folders specified according to the schedule you have chosen.

**3.0 How to Compress Your Backup File**

**Step 1**. Create a backup task as documented in section 2.3, containing the backup files you want to archive.

**Step 2**. Select “Archive” from the left sidebar to activate the *New task* screen as follows:



The **Compression** pane is used to specify the method for compressing your backup.

**Note**: Compression is used to reduce the amount of space for file storage. If you have a bunch of old files that you use only occasionally, but you still want to keep, it would make sense to store them in a format where they take up as little space as possible. Compression works by removing a lot of unnecessary coding out of your documents, while leaving important information intact. Compression does not damage your original data. The files are not viewable when compressed. The process must be reversed and your files 'decompressed' when you want to view the files again.

The three sub-options in the *Compression type* drop-down list are:

*No Compression*: This option does not perform any compression, as you would expect.

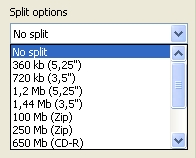
*Zip Compression*: This option is the standard compression technique for **Windows** systems, and the most convenient. Archives once created can be opened with standard Windows tools (or you can download the [**ZipGenius**](http://www.zipgenius.it/) program to access them).

Selecting a compression type listed automatically enables the *Split options* section, and its corresponding drop-down list.

The *Split options* apply to storage on removable media, for example CDs, DVDs, floppy disks and USB memory sticks. The various split options will subdivide the archive into sizes that will fit onto your storage device of choice.

Example: Let's say that you are archiving a large number of files, and you want to burn them to a CD. However, your archive size turns out to be larger than 700MB (the size of a CD). The splitting function will split the archive into pieces smaller than or equal to 700MB, which you can then burn onto your CDs. If you are planning to back up onto your computer's hard disk, or the files that you want to back up are smaller than the device you plan to store them on, you can skip this section.

The following options are available to you when you click on the *Split options* drop-down list. Your choice will depend on the type of removable storage device available to you.



* 3,5" - Floppy disk. This option is big enough to perform backup of a small number of documents
* Zip - Zip Disk (check the capacity of the one you are using). You will need a special Zip Drive in your computer and the custom-made disks
* CD-R - CD disk (check the capacity of the one you are using). You will need a CD Writer in your computer and a CD writing program (see [**DeepBurner Free**](http://www.deepburner.com/)version or other [**disk burning tools**](http://www.thefreecountry.com/utilities/dvdcdburning.shtml)).
* DVD - DVD disk (check the capacity of the one you are using). You will need a DVD Writer in your computer and a DVD writing program (see [**DeepBurner Free**](http://www.deepburner.com/)version or other [**disk burning tools**](http://www.thefreecountry.com/utilities/dvdcdburning.shtml)).

If you are backing up onto several USB memory sticks you may want to set a custom size.

To do this, perform the following steps:

**Step 1**. **Select** the *Custom size* (bytes) option, then type the size of the archive in bytes into the text field.

To give you an idea of sizes

* 1KB (kilobyte) = 1024 bytes - a one-page text document made in Open Office is approximately 20kb
* 1MB (megabyte) = 1024 KB - a photo taken on a digital camera is usually between 1 - 3 MB
* 1GB (gigabyte) = 1024 MB - approximately half hour of a DVD quality movie

**Note:** When choosing a custom size to split your backup for a CD or DVD disk, Cobian Backup will not copy the backup to your removable device automatically. Rather, it will create your archive in those files on the computer and you will need to burn them to the CD or DVD disk yourself.

*Password Protect*: This option lets you enter a password to protect the archive. Simply type, then re-type a password into the two boxes provided. When you try to decompress the archive, you will be asked for the password before the task commences.

**Note**: If you want to secure your archive, you should think about using another method than a password. Cobian Backup lets you encrypt your archive. This is covered below.

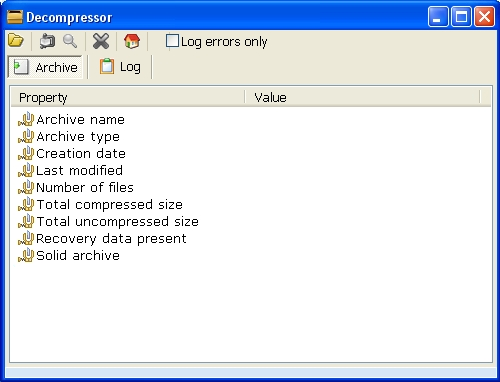
*Comment*: This option lets you write something descriptive about the archive, but it is not a requirement.

**3.1 How to Decompress Your Backup File**

To decompress your backup, perform the following steps:

**Step 1**. **Select > Tools > Decompressor**.

The Decompressor window appears as follows:



**Step 2**. Click on the open file icon to open a browse window to enable you to select the archive you want to decompress.

**Step 3**. Select the archive (*.zip* or *.7x* file) and then click “OK”.

**Step 4**. Select a directory into which you will unpack (output) the archived file.

**Step 5**. Click on the compression icon to open another window that lets you choose the folder in which to unpack the archive.

**Step 6**. Select a folder, and then click “OK”.

Use Windows Explorer to view the files that go to that folder.

**4.0 About Encryption**

Encryption may be a necessity for those wishing to keep their backup secure from unauthorised access. Encryption is the process of encoding, or scrambling, data in such a way that it appears unintelligible to anyone who does not have the specific key needed to decode the message. For more information on encryption, read the Protecting Files lesson.

**4.1 How to Encrypt Your Backup File**

The *Strong encryption* pane is used to specify the encryption method to be used.

**Step 1**. Click the *Encryption type* drop-down box to activate its list of different encryption methods.

To keep things simple, we recommend that you choose from either the *Blowfish* or the *Rijndael* (128 bits) methods. These will provide excellent security for your archive, and let you access the encrypted data with a chosen password.

**Step 2**. Select the *Encryption* type you want to use.

**Note**: *Rijndael* and *Blowfish* both offer approximately the same level of security. *DES* is weaker but the encryption process is faster.

**Step 3**. Type and re-type the password into the two boxes provided.

The strength of the password is indicated by the bar marked 'Passphrase quality'. The further the bar moves to the right, the stronger the passphrase. Refer to the **Passwords lesson** for information on creating and storing strong passwords.

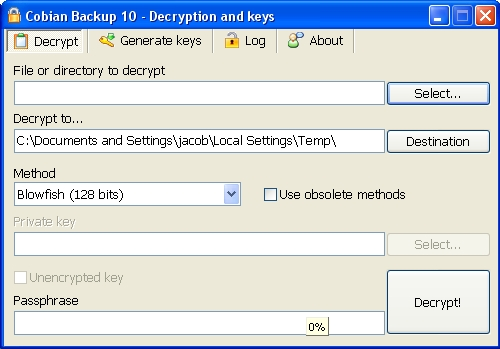
**Step 4**. Click “OK”.

**4.2 How to Decrypt Your Backup File**

Decrypting your backup file is easy and quick. To decrypt your backup file, perform the following steps:

**Step 1**. **Select > Tools > Decrypter and Keys**:

*This will activate the Decrypter and Keys window as follows:*



**Step 2**. Click “Select” to select the archive you want to decrypt.

**Step 3**. Click “Destination” to select the folder in which to store the decrypted archive.

**Step 4**. Select the same encryption type you selected earlier, in section 4.1 How to Encrypt Your Backup File, in the *Methods* drop-down list.

**Step 4**. **Select** the appropriate encryption method (the one you used to encrypt your backup file).

**Step 5**. Type your passphrase into the *Passphrase* text fields.

**Step 6**. Click “Decrypt!”

The file(s) will be decrypted to the location that you specified. If the files were also compressed, you will need to decompress them as outlined in section 3.1 How to Decompress Your Backup.