



USER MANUAL

v. 1.0.0.95 Windows Client

----- January 2014 -----

Contents

At a Glance

- 3 About SkyCrypt
- 4 About this manual

Getting Started

- 5 Download and install
- 6 Quick Start
- 7 SkyCrypt license

Basics

- 8 Creating a new drive
- 12 Connect to or restore existing SkyCrypt drives
- 14 Using SkyCrypt
- 16 Password settings

Advanced

- 17 2-factor authentication
- 21 Sharing encrypted files
- 22 Miscellaneous

Troubleshoot

- 23 FAQ
- 23 Contact support team

At a Glance

ABOUT SKYCRYPT

What It Is SkyCrypt is a file-based encryption program designed to secure your data before it is stored in the cloud.

Maximum Control & Security Using military-grade FIPS 140-2 validated 256-bit AES encryption, SkyCrypt protects your data with top-of-the-line technology. Moreover, since SkyCrypt encrypts files on your desktop, the information you place in cloud storage is safe from falling into the wrong hands even when...

- your cloud service provider is hacked at the root level, or
- your personal login to your cloud storage account is compromised

SkyCrypt ensures that YOU control access to YOUR data.

Easy to Use The DataLocker team designed SkyCrypt with intuitiveness in mind. SkyCrypt is one of the most user-friendly cloud storage encryption tools available today. Simply drag and drop your files into a SkyCrypt drive to seamlessly encrypt and decrypt your data in real time.

No Hassle SkyCrypt encrypts files individually, eliminating the task of resizing volumes. File-by-file encryption also ensures that your data can be synchronized and/or backed up problem-free.

ABOUT THIS MANUAL

The purpose of this manual is to provide instructions and guidance on how to utilize SkyCrypt and customize its settings to satisfy your encryption needs. Before using this guide, verify that your version of SkyCrypt and operating system match the title of this manual (see front page).

Mac OS is a registered trademark of Apple Inc.

Linux is a registered trademark of Linux Foundation.

The terms *Microsoft* and *Windows* used here are registered trademarks of Microsoft Corporation in the United States and other countries.

Note: this manual uses *Windows* to refer to...

- Microsoft® Windows® Millennium Edition
- Microsoft® Windows® 2000
- Microsoft® Windows® XP
- Microsoft® Windows® Vista
- Microsoft® Windows® 7
- Microsoft® Windows® 8

Getting Started

DOWNLOAD & INSTALL

Open your downloaded file of SkyCrypt to initiate the installation process. If you have not downloaded SkyCrypt, go to:

skycrypt.com → scroll to the bottom of the home page to either **Try** or **Buy**.

Installation

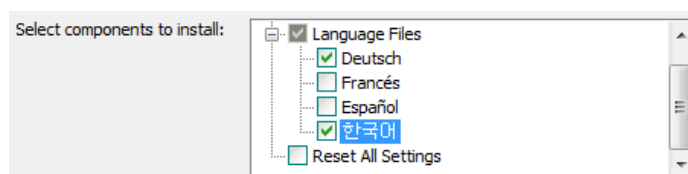
1. Use the dropdown menu to select your preferred language.

You may also change your language preferences under settings after you successfully install SkyCrypt.



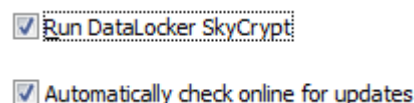
2. Review the license agreement. If you accept the terms of the agreement, select **I accept the terms of the License Agreement** and click **Next** to continue.

3. Check (uncheck) what you would like to install (not install). Then, click **Next**.



4. If you would like to change the destination folder for installing SkyCrypt, hit the **Browse** button. Otherwise, click **Install**.

5. You may start using SkyCrypt right after installing it onto your computer. Reboot is not required! Please leave the **Automatically check online for updates** box checked to receive SkyCrypt updates as soon as they become available.



Quick Start

SETUP Click the **New Drive** icon on the top left of the SkyCrypt screen. A setup wizard that will guide you step-by-step will appear. You will be asked to create a new SkyCrypt drive or connect to an existing one. If this is your first time using SkyCrypt, select **Create a new SkyCrypt drive** and then press **Next**.

STEP 1 The destination folder is where SkyCrypt will house all of the encrypted files that you store in your new SkyCrypt drive. To proceed:

- a. Select your desired cloud service provider
- b. Keep the preset path to the SkyCrypt folder or create a new custom path
- c. Keep the preset drive name or type in a new name

Memorize or write down the path to you encrypted folder to save yourself time in the future. Then, click **Next**.¹

¹ You must first install the client / application of your cloud service provider to sync it with SkyCrypt.

STEP 2 Establish your password for your new SkyCrypt drive. Your password needs to be at least 6 characters.

WARNING: SkyCrypt is zero-knowledge software, meaning that none of your passwords or personal information are stored. This also means that forgetting your password will render your data inaccessible!

After you create your password, we strongly suggest that you either write it down in a safe place or check the **Remember Password** option.

STEP 3 SkyCrypt uses a virtual drive system to instantly encrypt and decrypt your data. Select any of the drive letters that appear on the dropdown for your virtual SkyCrypt drive. Then, press **Next**.

Congratulations! You have completed the initial setup. Copy (or move) your files to the SkyCrypt drive to store your encrypted data in the corresponding SkyCrypt destination folder.

Before closing SkyCrypt, please backup your SkyCrypt security token – your encryption and decryption “key” - by saving the configuration file in a safe place on your computer (e.g., your encryption folder).

SkyCrypt License

All SkyCrypt users may enjoy the first 30 days of SkyCrypt for free under its 30-day free trial period. Once the 30-day trial expires, your SkyCrypt drives will operate in “read-only” mode. To continue use, you must activate the software.

Activation helps reduce software counterfeiting, ensuring that customers receive the software quality that they expect. Activation means that a specific product key becomes associated with the hardware it is installed on. Your SkyCrypt activation key can only be used one time and cannot be used to activate SkyCrypt on other computers.

To retrieve your SkyCrypt activation key, click on the link below...

[Buy SkyCrypt Online](#)

Add SkyCrypt to your shopping cart and checkout. Once you have paid for the product, you will receive your activation code via e-mail.

1. Copy your activation key
2. Open the SkyCrypt application
3. Click on the **Activate** button located on the toolbar



4. Enter your product key
5. Click **Next** to activate your perpetual license of SkyCrypt and resume using its features

Basics

Create a New Drive

SkyCrypt can be used to protect your files on any cloud storage provider that can be integrated with Windows.

If you use multiple cloud service providers and would like to sync SkyCrypt to each of your cloud storage accounts, you will need to create a SkyCrypt drive for each client. If you do not have a cloud storage client or application for your cloud storage provider downloaded on your computer, SkyCrypt will not automatically sync and upload your encrypted files to your cloud account.

If you do not already have a cloud storage client installed, click on the link(s) of your cloud storage provider below. You will be taken to their download page.



[Bitcasa](#)



[Box.com](#)



[Dropbox](#)



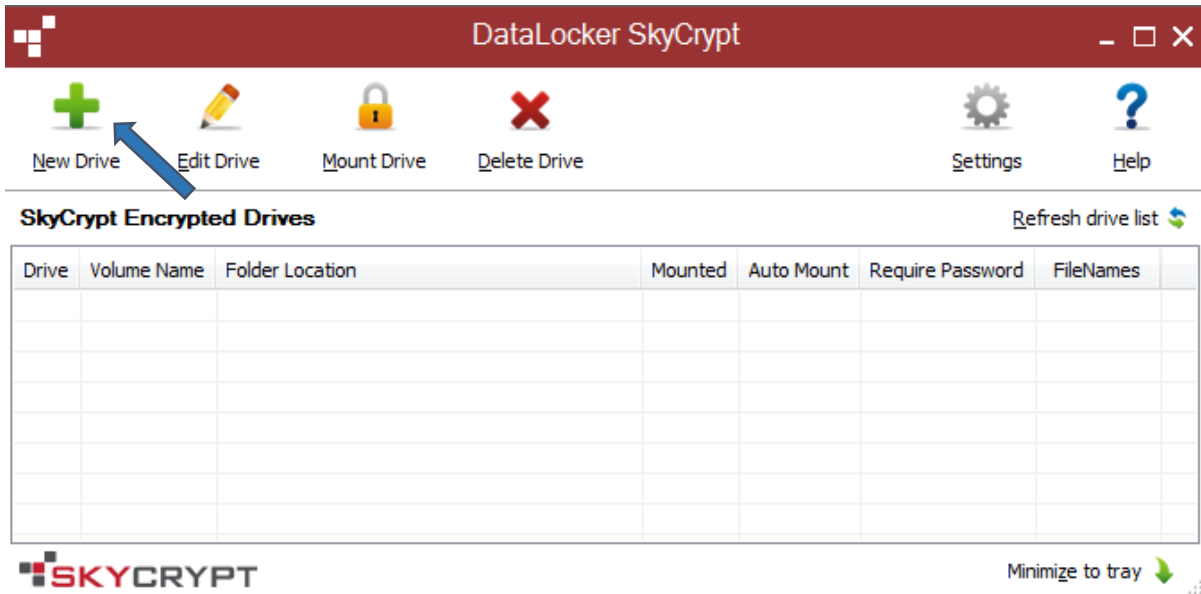
[Google Drive](#)



[SkyDrive](#)

Once you have your desired cloud storage client(s) installed onto your computer, you can add a virtual SkyCrypt drive that will encrypt your files and sync them automatically with your cloud storage provider.

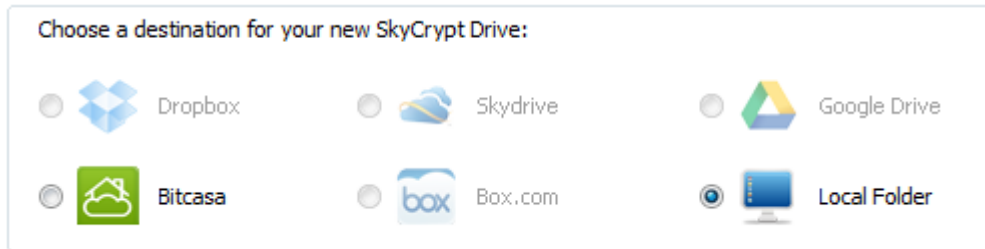
To get started, click the **New Drive** icon on the top left of the toolbar.



You will be prompted to either create a new SkyCrypt drive or connect to an existing one. If this is your first time using SkyCrypt, please select **Create a new SkyCrypt drive** and then press **Next**.



STEP 1 You will then be asked to choose a destination folder for your new SkyCrypt drive.



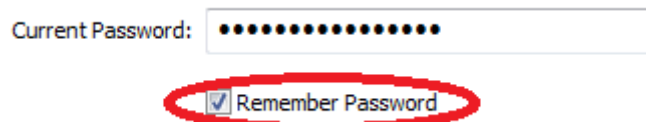
The destination folder is where SkyCrypt will house all of the encrypted files that you store in your new SkyCrypt drive. To accomplish this:

- a. Select your desired cloud service provider.
- b. Keep the preset path to the SkyCrypt folder or create a new custom path.
- c. Keep the preset drive name or type in a new name.

Click **Next** to continue.

STEP 2 Establish your password for your new SkyCrypt drive. Your password needs to be at least 6 characters. We recommend that you create a strong password, including 8 or more characters and multiple numbers and symbols.

WARNING: To ensure the security of your files, DataLocker does not store your SkyCrypt passwords. This also means that forgetting your password will render your data inaccessible.



After you create your password, we strongly suggest that you either write it down in a safe place or check the **Remember Password** option.

STEP 3 SkyCrypt uses a virtual drive system to both encrypt and decrypt your data. When you drop files into the SkyCrypt drive, SkyCrypt will encrypt those files and then store them in the destination folder that you set in Step 1.

You can also view (decrypt) the encrypted files that are in your destination folder by accessing your virtual SkyCrypt drive.

Assign this drive letter to your new SkyCrypt Drive: Y: ▼

Advanced Options

Enable Auto Mount
This drive is automatically mounted and active when SkyCrypt starts up.

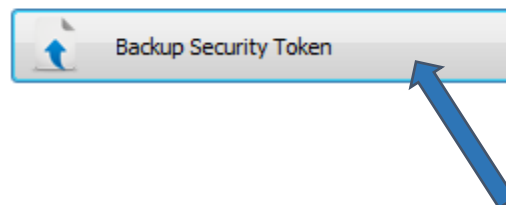
Enable File Name Encryption
File name encryption makes all your file and folder names unreadable outside of SkyCrypt.

Assign any of the drive letters that appear on the dropdown for your virtual SkyCrypt drive. Then, press **Next**.

Congratulations! You have completed the initial setup. Copy (or move) your files to the SkyCrypt drive to store your encrypted data in the corresponding SkyCrypt destination folder.

Before closing SkyCrypt, please backup your SkyCrypt security token – your encryption and decryption “key” - by saving the configuration file in a safe place on your computer (e.g., your new encryption folder).

**** Strongly Recommended! Backup your encryption key file that is linked to this SkyCrypt Drive. This security token file holds all the required encryption information for encrypting and decrypting your data. If this file is lost or corrupted you will not be able to access your data!**



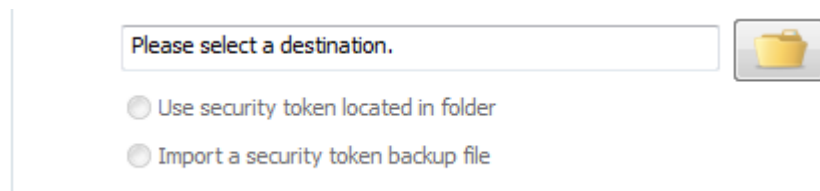
Connect to or Restore an Existing SkyCrypt Drive

You can use SkyCrypt to access your encrypted data on more than one computer. To access an encrypted folder on a different computer through SkyCrypt, click on **New Drive** to open the SkyCrypt setup wizard.

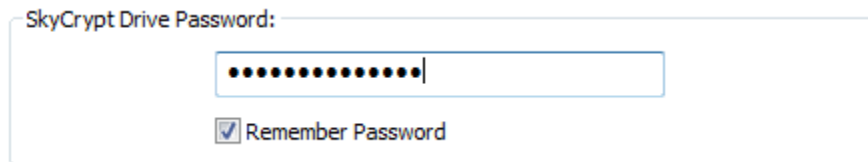
Next, pick the option, **Connect to or restore an existing SkyCrypt Drive**.



STEP 1 Select the location of the encrypted folder. Click on **Browse** and highlight the already existing encrypted folder. Then, click **Next**.

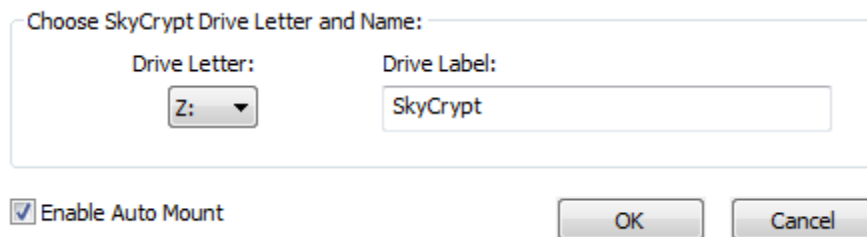


STEP 2 To access data in the already existing encryption folder, you must type in the password that was originally used to encrypt the files. After you correctly type in the password, you can check **Remember password** if you do not want to re-type the password every time.



The screenshot shows a dialog box titled "SkyCrypt Drive Password:". It contains a text input field with a password represented by 12 black dots. Below the input field is a checked checkbox labeled "Remember Password".

STEP 3 Choose one of the available drive letters to establish the virtual drive through which you will encrypt and decrypt your files.



The screenshot shows a dialog box titled "Choose SkyCrypt Drive Letter and Name:". It has two input fields: "Drive Letter:" with a dropdown menu showing "Z:" and "Drive Label:" with a text input field containing "SkyCrypt". Below these fields is a checked checkbox labeled "Enable Auto Mount". At the bottom right are "OK" and "Cancel" buttons.

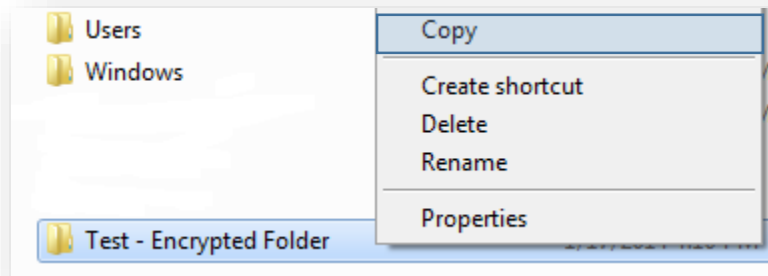
Congratulations! You can now access your encrypted data on another computer. Simply repeat these instructions to access your already-encrypted data on other computers.

Using SkyCrypt

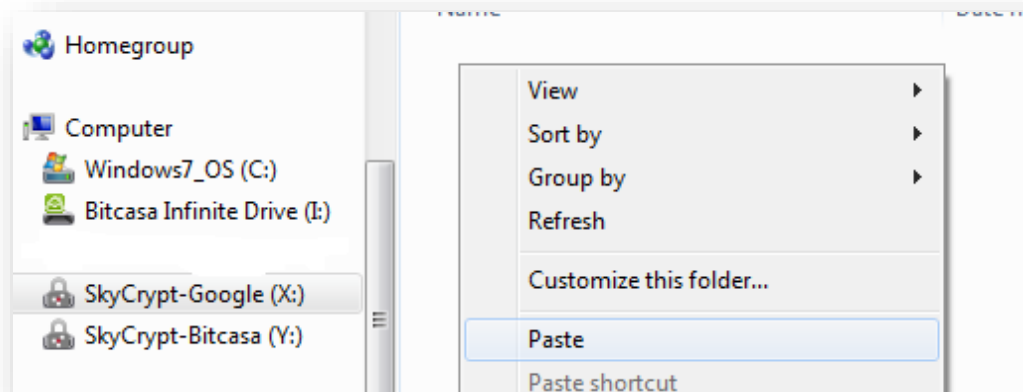
The SkyCrypt drive is functionally the key through which you can encrypt and decrypt all of your data. Your SkyCrypt drive can be implemented as either a hard drive or a network drive. Open **My Computer** by clicking on the Windows start ribbon to see if your virtual SkyCrypt drive is contained a synchronized folder or a network drive.

HOW TO ENCRYPT YOUR DATA

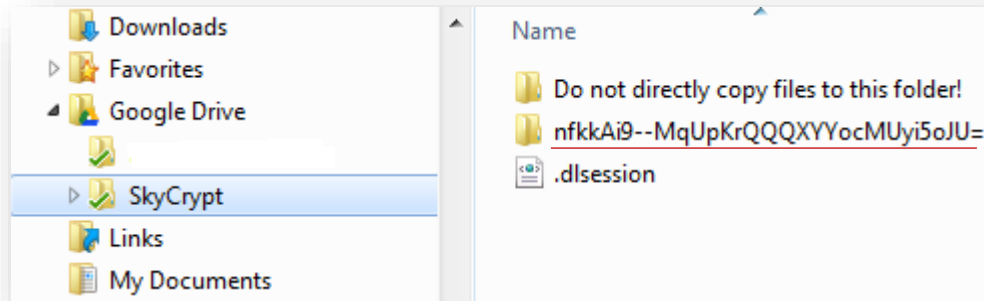
Highlight the files / folders that you want to encrypt.



Then, copy (or move) them into your desired SkyCrypt drive.

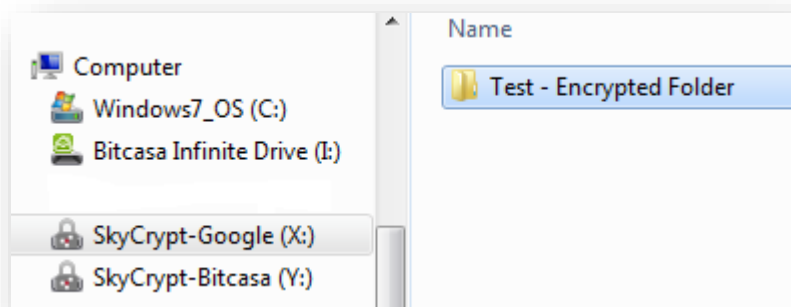


SkyCrypt will encrypt the files that you drop into the SkyCrypt drive and upload the now encrypted files to your cloud storage account.



HOW TO DECRYPT YOUR DATA

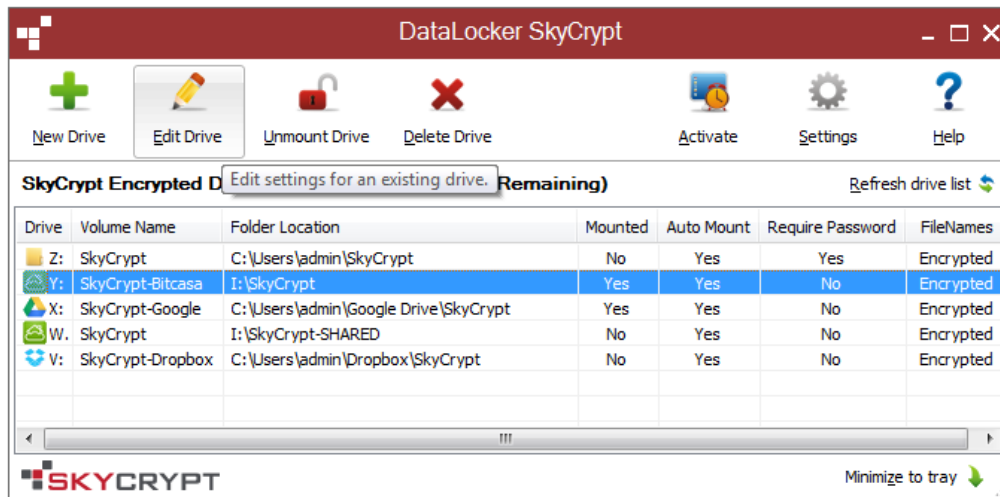
Your files can only be decrypted when SkyCrypt is open on your local machine. Simply go to your SkyCrypt drive to view your decrypted data. You can open and edit the files and folders on your SkyCrypt drive as you would with any other file on your computer.



Password Settings

At any time, you can edit whether or not you want to require a password for your SkyCrypt drive.

If you want your SkyCrypt drive to require a password, highlight the drive on your SkyCrypt screen and click **Edit Drive** on the toolbar.



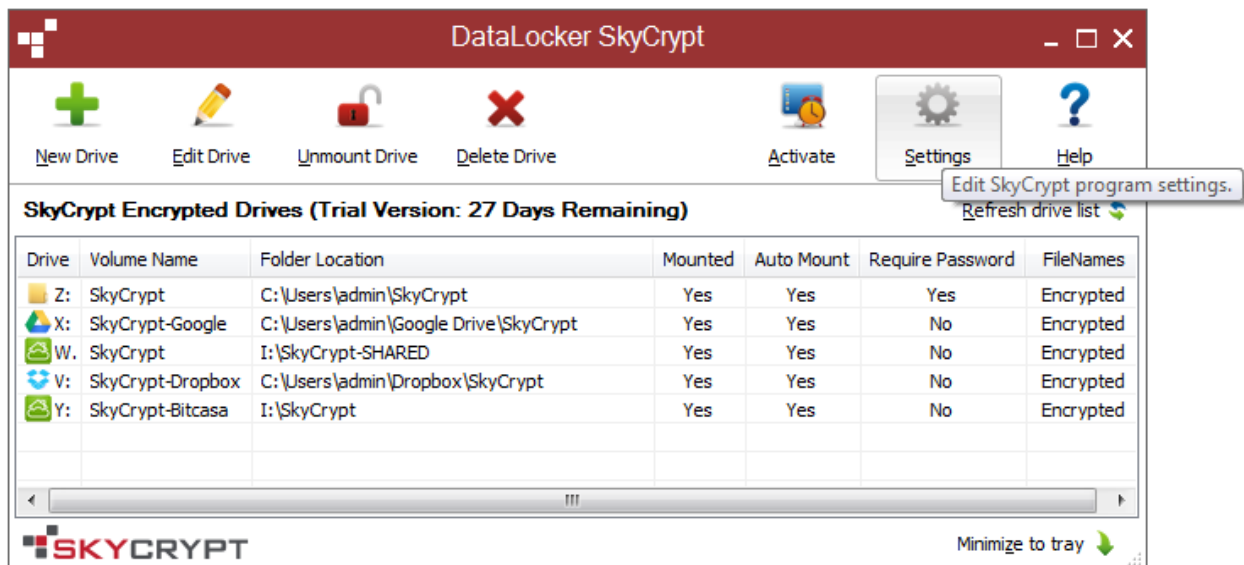
Uncheck the **Remember Password** box. Your drive will now require a password and reset to the password that you most recently inputted. If you would like to change your password, click on the **Change Password** box, and fill in the fields below.



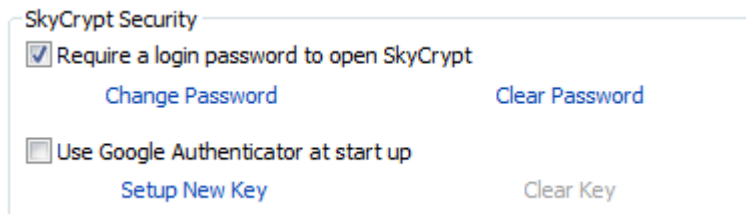
After you have changed the password settings, click **OK**. Now, you will be prompted to enter a password for the SkyCrypt drive that requires a password. To apply this setting, you must exit and reopen SkyCrypt, or you can un-mount and re-mount the SkyCrypt drive on the main window.

Set a Password for SkyCrypt Application

You can also require a login password for the SkyCrypt program. To accomplish this, click on **settings** on the toolbar.



Check the **Require a login password to open SkyCrypt** box. Then, after entering and / or changing your password, hit **OK**.



Warning: The next time you open SkyCrypt, you will be required to enter a login password. Lost or forgotten passwords CANNOT be recovered.

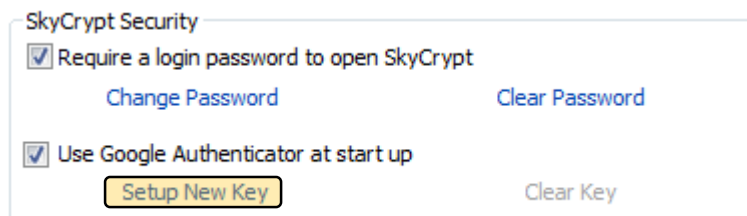
Advanced

2-Factor Authentication

Enable 2-factor authentication for an added layer of security. To pair your mobile device, click on [Settings](#).



Check the [Use Google Authenticator at start up](#) option and click [Setup New Key](#).



STEP 1 The Google Authenticator setup instructions will appear. To continue, you will need to install the Google Authenticator app on your mobile device.

iPhone, iPad, iPod Touch

Visit the App Store and search for Google Authenticator.

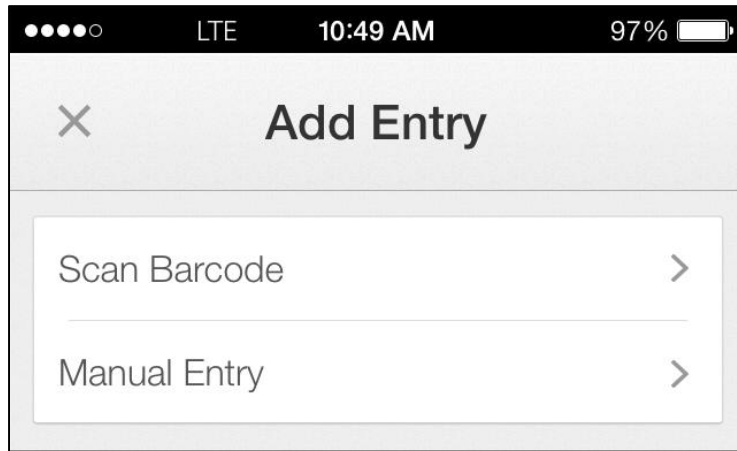
Android

Visit Google Play and search for Google Authenticator.

BlackBerry

Visit www.m.google.com/authenticator on your web browser.

STEP 2 Open the Google Authenticator app on your phone and select **Scan Barcode**.



Use your camera to scan the barcode on the setup screen. If you are unable to scan the barcode, select **Manual Entry** and enter the appropriate fields on Google Authenticator.

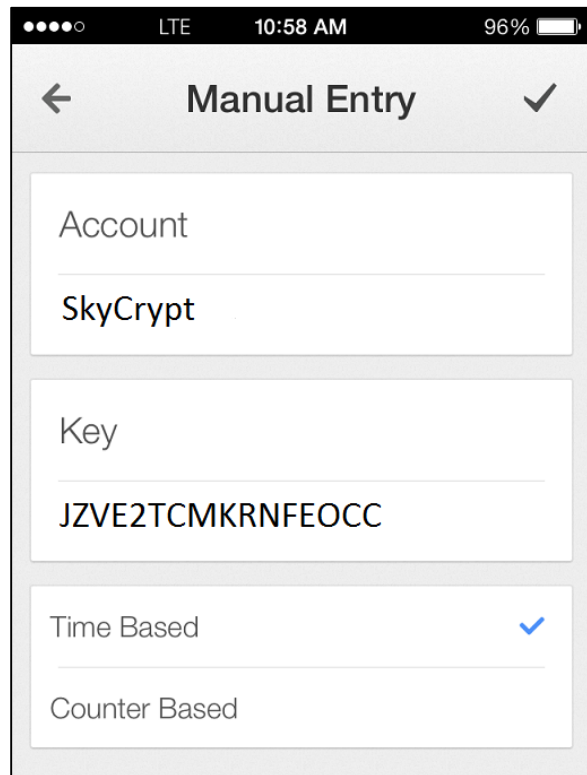
2. Scan the barcode below using the Google Authenticator app on your mobile device.

Generate new Google Authenticator secret key

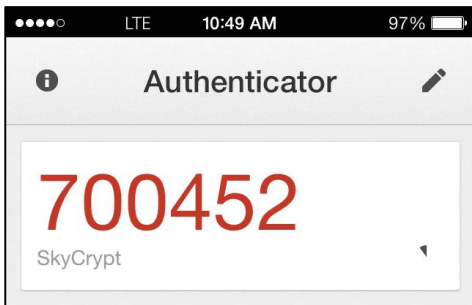


Use the settings below, If you are unable to scan the barcode.

Account: Key:



STEP 3 Enter the authentication code that appears on Google Authenticator to the verification field.² Then, hit **OK** to save your settings.



3. Verify that the pairing was successful by entering a passcode below:



² Google authentication codes expire in 30 seconds. Your code will turn red when fewer than 5 seconds remain.

Right-click **Minimize the tray** and then **Exit SkyCrypt**. When you reopen SkyCrypt, it will now require your Google Authentication key.



Open Google Authenticator, and type in the code that appears under your SkyCrypt account to log in to SkyCrypt.

Sharing Encrypted Files

Sending an Encrypted File

To send a SkyCrypt-encrypted file to another SkyCrypt user, share the encrypted file / folder as you normally would using your cloud service provider. To ensure that the recipient will be able to access and decrypt your shared document(s), you must also send...

- the security token (look for an .XML file), and
- your virtual drive password

Otherwise, the recipient will not be able to view your encrypted file(s).

Receiving and Decrypting a Shared Encrypted File

To decrypt a SkyCrypt-encrypted file that has been shared with you, first make sure that the shared file is present in your cloud storage client. Then, follow these instructions:

1. Click on **New Drive**.
2. Select **Connect to or restore an existing SkyCrypt drive**, then hit **Next**.
3. Search for the encrypted file that has been shared with you by clicking the **Browse** button.



Select the shared encrypted file, then hit **OK**.

4. If the security token is in your shared file, you will receive a message that says, **Existing security token found!** Select **Use security token located in folder**. If you saved the security token elsewhere, then import it by browsing your files for the key.
5. Enter the SkyCrypt drive password that you retrieved from the sender.
6. Choose an available drive letter and name the new drive. Then hit **Next**.

Use your new virtual drive to view the decrypted data.

Miscellaneous

Deleting a Drive

Highlight the drive that you want to remove and press the **Delete Drive** button. You will then be asked if you want to permanently delete your files as removing the drive will not delete the encryption folder and its contents.

Mounting a Drive

You need to mount a drive in order to access it on your computer. Highlight the un-mounted virtual drive on your SkyCrypt app, and then hit **Mount Drive**.

Note: you can only mount one drive with the same assigned drive letter at a time.

Un-mounting a Drive

If you need to reboot a particular SkyCrypt drive after changing its settings, you can un-mount (then re-mount) the drive on your SkyCrypt application. To un-mount the drive, highlight the mounted virtual drive, and then hit **Unmount Drive**.

You can also un-mount a drive to free up memory on your computer or free up a drive letter.

Default Drive Settings

To change the default settings for your virtual drive, select the SkyCrypt drive and click **Edit Drive**.

- Enable Auto Mount: This feature will automatically mount your drive when you log in to SkyCrypt.
- Enable Long File Names: This feature supports paths that are longer than 260.
- Enable File Name Encryption: This feature will encrypt the names of all of your files and folders. Unchecking this feature will reveal the names of your files and folders, although its contents will remain encrypted.

Auto Mount Options:

Enable Auto Mount

Delay Drive Auto Mount: Seconds

File Name Options:

Enable Long File Names

Enable File Name Encryption

Add File Name Extension (.sky)

Enable Case-Insensitive File Names

Troubleshoot

Frequently Asked Questions

Because SkyCrypt is still relatively new, there are no FAQ's at this time. Please contact the DataLocker SkyCrypt support team for technical help. We will begin adding FAQ's once we receive enough questions about a specific issue.

Thank you for understanding. 😊

Contact the Support Team

If you have any unresolved issues with our software after referring to this manual, give us a call or go to our website to chat with a DataLocker representative.

Phone: (913) 310-9088

Web: datalocker.com

If you would like to contact us outside of our business hours (8:30AM – 5:30PM CST), visit our support page to post your question, and we will get back to you as soon as possible.

Support Site: support.datalocker.com/customer/portal/questions/new