Introduction

What is the Cloud?

> There is no cloud. It's just someone else's computer.

Mobile devices and cloud storage fundamentally changed the way we work with files. Files must be **available** on all devices and for everyone who needs access. Providers, such as Dropbox, OneDrive or Google Drive, fulfill this need by organizing the storage of your files for you. They store **your files on their servers**, and sync them to every connected device.

While the cloud offers many advantages, such as automatic backups or a reduction of costs for hardware, you pay with **losing control over your data**. Everyone who has access to the cloud provider's server can read your files.

What is Boxcryptor?

Boxcryptor provides a **user-friendly**, additional layer of security for cloud storages by **encrypting files locally** on your device. Since Boxcryptor was **optimized for the cloud** from the very beginning, the encryption takes place on **every file** and access can be shared. This means that every file is encrypted **independently** from the others.

What Boxcryptor is **Not**

- Boxcryptor is **not a cloud storage service**. It is a security software that adds a security layer to the cloud storage of your choice. Therefore, Boxcryptor does not store your data. The responsibility of storing and managing your files lies at your cloud provider.
- On **Windows**, Boxcryptor is **not a sync client**, which means that it does not synchronize your files to the cloud. This responsibility also lies at your cloud provider. Therefore, you have to install your cloud provider's software on your device.

- Boxcryptor is **not designed to secure arbitrary cloud services**. Services such as Google Docs or Evernote do not work with locally stored files, but store the data directly in databases on their servers. Boxcryptor can only encrypt files – your files that you store in your cloud – not services.
- Boxcryptor is **not a VPN solution**. Although we have partnerships with various VPN providers, we are in no way technically connected to their products.

Quickstart

Are you ready to secure your cloud storage? This guide helps you to get started with Boxcryptor and your cloud storage service.

Install Boxcryptor

To install Boxcryptor, download the desired version from our Website.

ℹ On first start, Boxcryptor will ask you to finish the installation by entering the credentials of your **macOS account** with admin privileges. These are **not** your Boxcryptor credentials.

Installation Instructions for Boxcryptor (3.x)

Required macOS Version:

- Requires **macOS 12.0** or later. Please note that we do not officially support beta versions of macOS. New versions of macOS, however, will be supported by Boxcryptor as soon as they have been officially released by Apple, sometimes even a bit in advance.

File Synchronization:

- Boxcryptor 3.x **includes the full functionality for fast, smooth and secure synchronization of your files and folders.** It is all you need installed on your Mac to work with encrypted files in Dropbox, OneDrive, Google Drive or any other supported cloud provider. You can remove your cloud provider's client from your Mac.

Security :

- Boxcryptor 3.x is a native "File Provider" app which works "out-of-the-box" on modern macOS operating systems. Additionally, the app is fully utilizing the macOS sandboxing security mechanism.

Encryption of locally stored files:

- **Files stored locally on your Mac are not encrypted by Boxcryptor anymore due to technical limitations by Apple's File Provider platform.** File Provider apps must store files in cleartext on the local filesystem so that their content can get picked up by macOS and presented to the user. This affects file contents and file names.
- Here's the encryption state by location:
  - **In the cloud:** Files are always protected by Boxcryptor's encryption
  - **On your Mac with FileVault:** Files are protected by FileVault's encryption
  - **On your Mac without FileVault:** Files are not protected (not recommended)
- **We strongly recommend the use of local full-disk encryption for every Mac** – regardless if

you are using a previous version of Boxcryptor for macOS or the new Boxcryptor for macOS Beta or even if you don't use Boxcryptor at all. Full-disk encryption is an integral part of local device security and can easily be achieved by turning on FileVault on any Mac.

By using **FileVault**, files available in the new Boxcryptor for macOS Beta are still protected by FileVault's encryption on the local disk despite appearing as cleartext when your Mac is in use. Learn more about FileVault here: https://support.apple.com/en-us/HT204837

Spotlight:

- A major advantage of the File Provider-API is that Spotlight works out-of-the-box without requiring special handling by Boxcryptor. This means that **Spotlight indexes visited files and folders in Boxcryptor locations automatically and by default.** Spotlight support is not an optional advanced setting anymore, but a first-class default experience for every user.

› Installation Instructions for Boxcryptor 2.x (legacy)

Create a Boxcryptor Account

With Boxcryptor joining Dropbox, we do no longer allow new accounts to be created.

We strive to make managing encrypted files as simple as possible. Just set up your Boxcryptor account and we handle all the difficult operations that come with encryption for you.

1. Start **Boxcryptor**.
2. Click on **create account**.
3. Follow the wizard to finish the account creation.

Create a password that you can remember, or store the password in a secure place, for example a password manager. Boxcryptor is a zero knowledge encryption software, therefore we **cannot** restore your password.

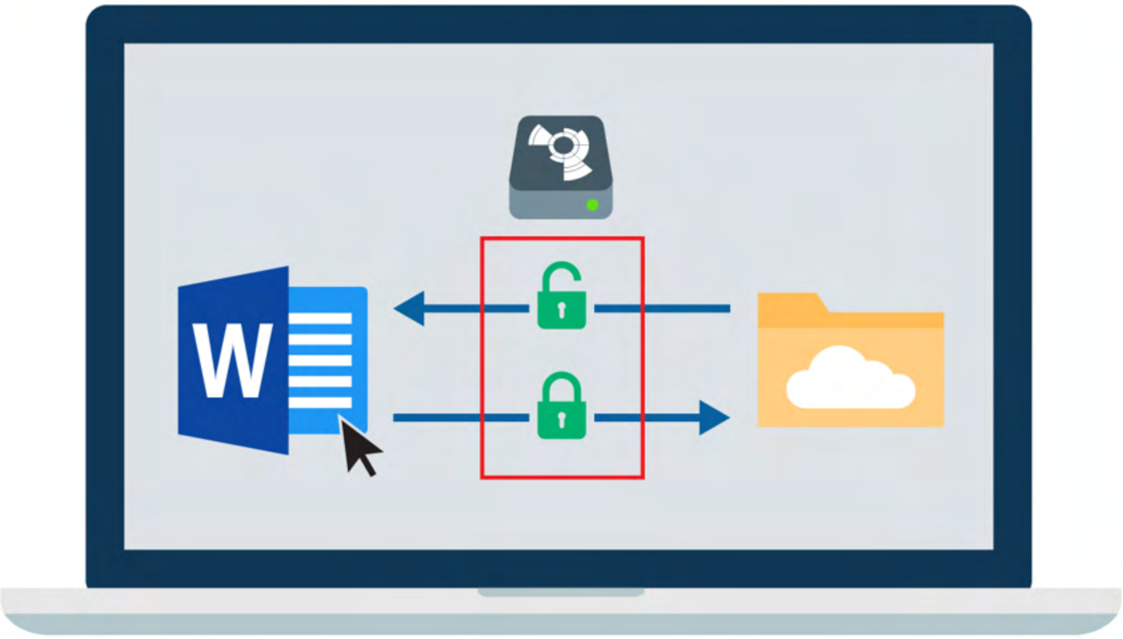
If you lose your password, your data will be lost irrevocably.

Due to restrictions from Apple, it is not possible to create a Boxcryptor account within the macOS app. Before using Boxcryptor for macOS, you must first create your account on our web interface.

Discover Boxcryptor

Once you have installed Boxcryptor and signed in with your account, you can add your cloud provider and start browsing your files.

From now on, you can use Boxcryptor to work with your files in the cloud. The app connects with your cloud provider and takes care of uploading and downloading files, as well as decryption.



Small icons mark the files, and show you whether a file or folder is encrypted 🔒 or not.

You can open the Boxcryptor App by clicking on the Boxcryptor logo in your menu bar. To browse your cloud provider locations, either click the requested location here or open the Finder and go to the **Location** section in the sidebar.

Your First Encrypted Folder

All files and folders that you add in Boxcryptor will be **encrypted automatically**. If you are new to Boxcryptor and do not have any files in your cloud yet, this is how you get started.

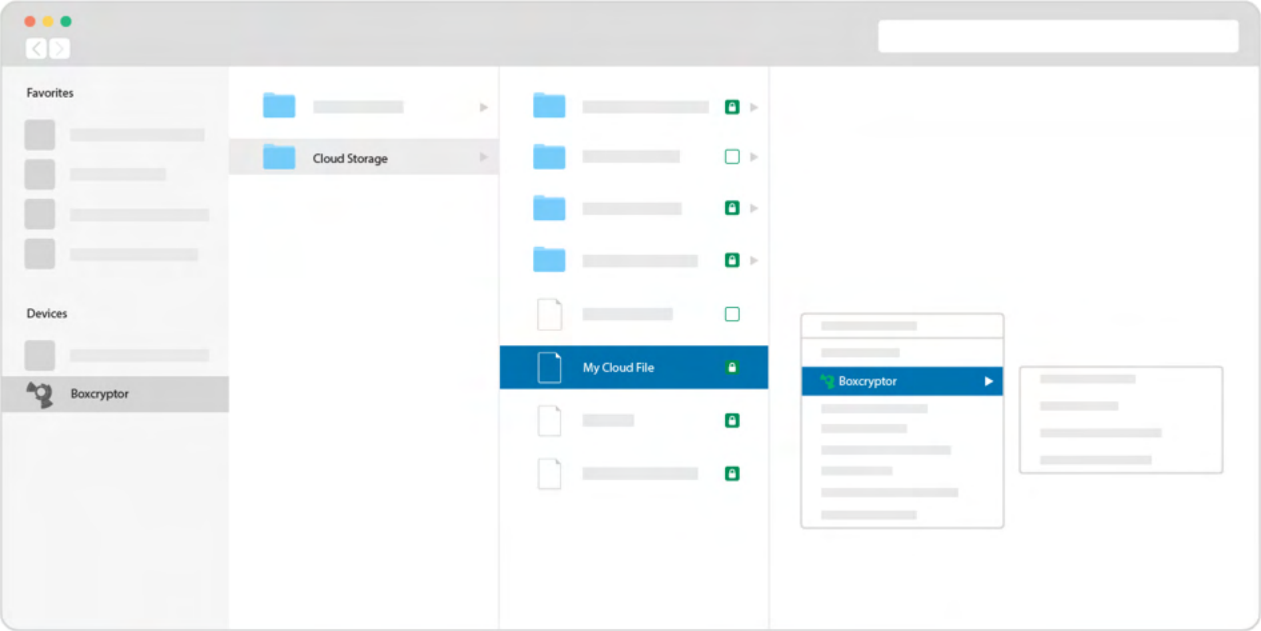
1. Open the **Boxcryptor Location** of your cloud provider.
2. Click on ⋯ → **New Folder**.
3. Add files to the folder and all files will be encrypted automatically, inheriting all permission and encryption properties.

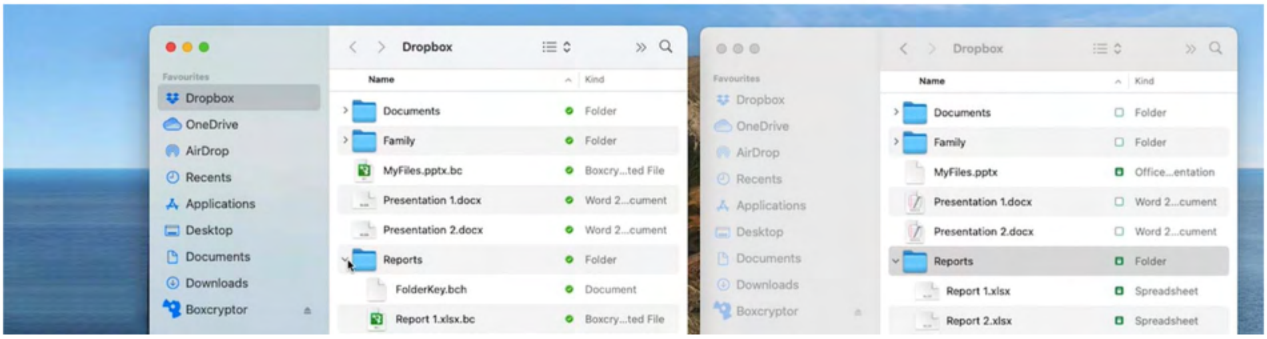
How to Encrypt Existing Files

If you already have files and folders in your cloud, Boxcryptor can encrypt these existing files as well.

1. Go to your **Boxcryptor Location**.
2. **ctrl-click** on a file or folder → **Create Encrypted Copy**.
3. Select the appropriate permissions and confirm the operation.

Boxcryptor will then create an encrypted copy of your selection and automatically upload it to your cloud-provider.



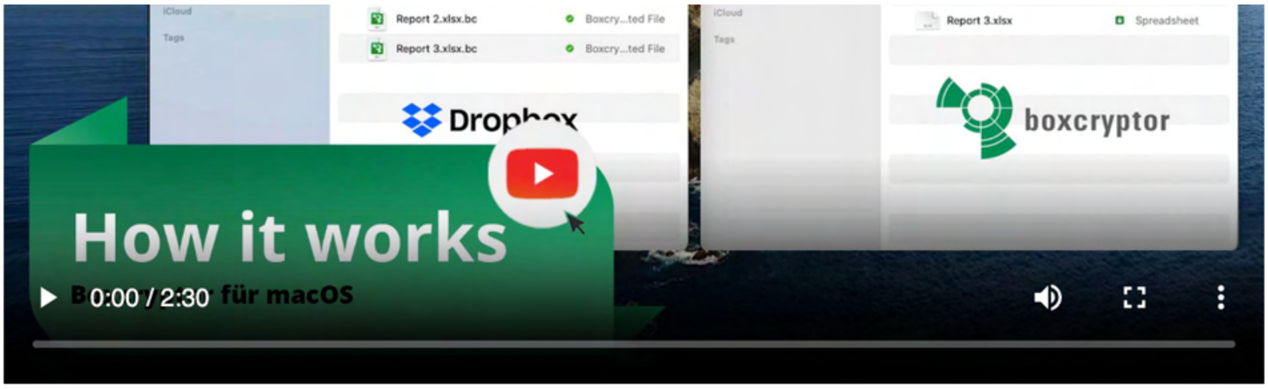


Dropbox

Name		Kind
Documents	●	Folder
Family	●	Folder
MyFiles.pptx.bc	●	Boxcry...ted File
Presentation 1.docx	●	Word 2...cument
Presentation 2.docx	●	Word 2...cument
Reports	●	Folder
FolderKey.bch	●	Document
Report 1.xlsx.bc	●	Boxcry...ted File

Dropbox

Name		Kind
Documents	□	Folder
Family	□	Folder
MyFiles.pptx	■	Office...entation
Presentation 1.docx	□	Word 2...cument
Presentation 2.docx	□	Word 2...cument
Reports	■	Folder
Report 1.xlsx	■	Spreadsheet
Report 2.xlsx	■	Spreadsheet



iCloud
Tags
Report 2.xlsx.bc
Boxcry...ted File
Report 3.xlsx.bc
Boxcry...ted File
Dropbox
iCloud
Tags
Report 3.xlsx
Spreadsheet
boxcryptor
How it works
Boxcryptor für macOS
0:00 / 2:30

Manage Clouds and Locations

Boxcryptor supports a vast variety of cloud storage providers out of the box. Additionally, Boxcryptor works with every cloud provider which supports the WebDAV protocol.

Add Provider

Boxcryptor works as an **additional security layer** for your cloud storage. On macOS, we **connect directly** to your provider and handle both uploading and encrypting your files. To add a new provider to Boxcryptor, follow these steps:

1. Open the **Boxcryptor app** and navigate to **Home**.
2. Click on **Add Provider** and select your provider.
3. Allow Boxcryptor to sign in to your provider and complete the authentication process.

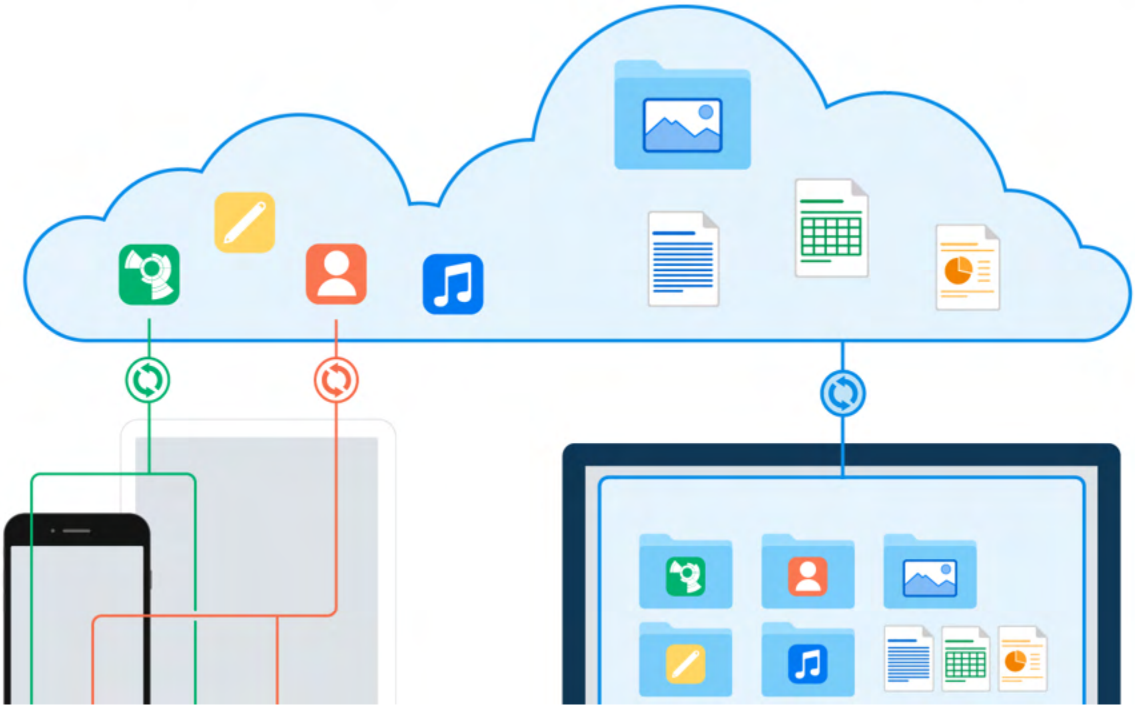
> ⓘ You can also **rename** or **delete** your provider with ctrl-click.

Google Drive

Boxcryptor gives you access to files stored in Google Drive's **My Drive**, **Shared Drives** and **Shared_. Additional folders backed up via** My Computer_ *are _not* available.

iCloud

Due to technical restrictions by Apple, Boxcryptor for macOS differentiates between **iCloud** and **iCloud Drive (Mac & PC only)**. If you plan to use Boxcryptor on your iPhone or iPad as well, make sure to use **iCloud**, because **iCloud Drive (Mac & PC only)** is only available on Mac or PC devices.



Make sure to use the same Apple ID on your iOS device and your Mac.

Custom Locations

Boxcryptor supports adding folders of your local file system as **Local Storage** provider:

1. Open the **Boxcryptor app** and navigate to **Home**.
2. Click on **Add Provider** and select your provider.
3. Click on **Local Storage** and choose your own, customized location.

If your chosen location is not a sync folder of a cloud provider, nothing will be uploaded to the cloud. The data stays on your PC locally, just like any other folder, but encrypted.

WebDAV Locations

If your cloud provider is not listed as a supported provider, chances are high that Boxcryptor supports it nevertheless, because we support the **WebDAV** protocol. This protocol is used by most providers.

1. Contact your cloud provider for the WebDAV credentials.

Boxcryptor requires a secure server connection (`https://`) with a valid or self-signed SSL certificate installed on the device.

In local networks, IP-based unencrypted connections (`http: //`) are also possible, provided you allow this on your device.

2. Open the **Boxcryptor app** and navigate to **Home**.
3. Tap on **Add Provider** and select **WebDAV**.
4. Complete the authentication process with the given WebDAV credentials

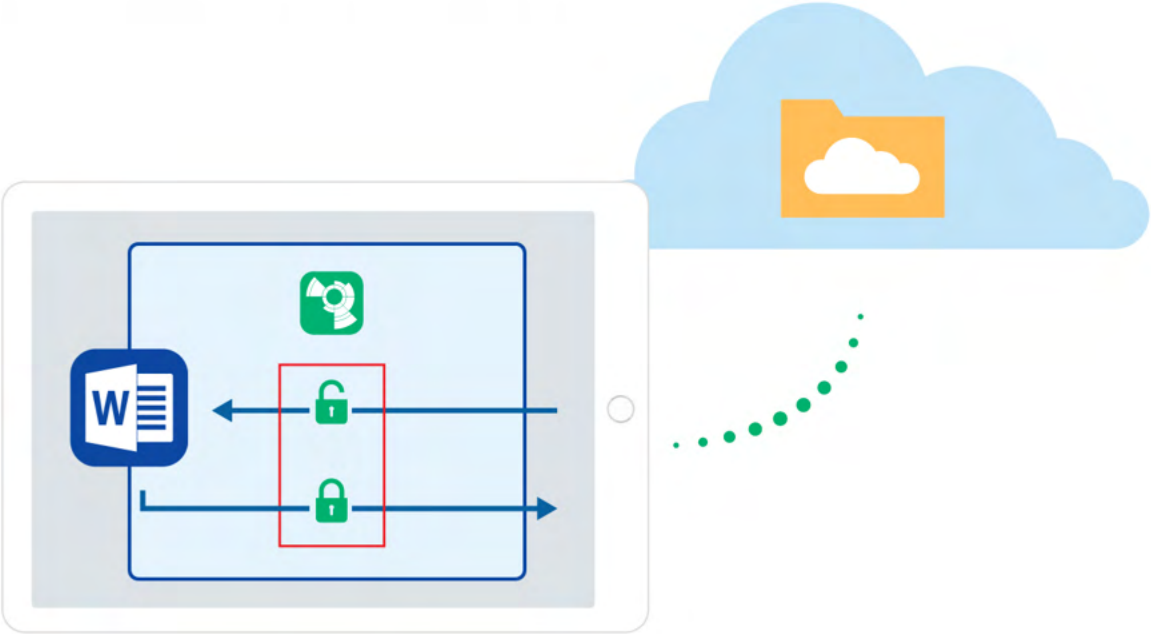
ownCloud and nextCloud both support WebDAV. By default, the configuration URLs are:
`https://example.com/owncloud/remote.php/webdav` *and*
`https://example.com/nextcloud/remote.php/dav/files/username/`

Work With Files

We focus on designing Boxcryptor as **user-friendly and easy to use** as possible. Once Boxcryptor is set up, you will not notice that your files are encrypted. Just keep working with your files as usual.

On-the-fly Encryption

Boxcryptor encrypts your data **on-the-fly** and it encrypts **every file separately**. When you work with your files there is no need for bulk decryption. You can just open any encrypted file and it's content will be decrypted automatically in the background. When you save your changes, the contents are encrypted automatically again. Simply work with your protected data with Boxcryptor without noticing the cryptographic process behind it.

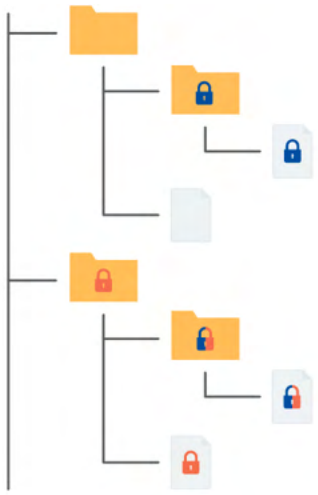


We decrypt and encrypt your files on demand: Do you want to view your content? Just click on it and we download and decrypt your file for you. Are you finished with writing your essay? Just save it to Boxcryptor and we encrypt the file and store it into the cloud.

Encryption and Permission Hierarchy

You can decide for every file or folder which security level you want to set. Boxcryptor gives you **full control** over this. You can allow others to access a file by giving permissions, you can choose if the filename should be encrypted as well, or you can leave single files and folders unencrypted.

To make things easier **all properties of a file are inherited hierarchically from its containing folder**. For example, if you have an encrypted folder called *My Secret Files* and add a file to this, the file will be encrypted automatically and the chosen permissions will be inherited. The same applies to whole folders.



🔒 **Encrypted** and **permission to access** for **Alice**

🔒 **Encrypted** and **permission to access** for **Bob**

🔒 **Encrypted** and **permission to access** for **Alice and Bob**

Note: If you add a file to a folder that is not encrypted, Boxcryptor will automatically encrypt it.

Work With Your Files

With Boxcryptor, you **never need to manually decrypt** any data when you want to work with it.

Boxcryptor deeply integrates into macOS and can be found directly in the **Finder** under **Locations** . The encryption takes place on-the-fly. Therefore, all other programs, including the Finder, will work the **same way as with files on your hard drive**.

To work with your encrypted files, just browse to the Boxcryptor Location in **Finder** and edit, view, copy, or move files as in any other folder.

ⓘ If you do not have Boxcryptor permissions to open a file, some programs will show errors like "cannot open" or "Error code -36". In such a case, verify that you have the permission to open the file via ctrl-clicking the **file or folder** → **Manage Permissions**. See Share with Boxcryptor users for more info.

How to Recognize Encrypted Files

Boxcryptor allows you to have **encrypted and unencrypted** files and folders. Encrypted files or folders in the Boxcryptor location are **marked with small icons**.

🔒 **encrypted**

Encrypt Existing Files and Folders

If you already have files stored in your cloud, you can encrypt your existing files as well. This is how it works:

- Browse to the file or folder you want to encrypt.
- Ctrl-click the selection and chose **Create Encrypted Copy** in the context menu.
- Wait for Boxcryptor to sync everything.

Work With Filename Encryption

Filename encryption effectively **prevents outsiders from analyzing** your data structure. However, it also comes with the cost of a slightly **slower performance** and higher efforts regarding a proper setup. If you want to use filename encryption with shared files and folders, please read our blogpost, especially **chapter 5**, before proceeding.

> A filename encrypted file will look like this: 恂悰挦抱砻抮殯枏瞻擟敳漢快搬濂檬浉楻挭抧柜欅䀣.bc

Filename encryption can be **enabled globally**. All new encrypted items that do not inherit encryption settings from their parent folders will be encrypted with filename encryption. Existing encrypted files, however, will not be touched, which means that you have to activate filename encryption for existing files manually. Filename encryption is one of the properties that **files inherit** from their parent folder. Therefore, if you save a file to a folder with filename encryption, it will have filename encryption as well.

> Conclusively, even if filename encryption is enabled globally, new files that are created in a folder *without* filename encryption will also have *no* filename encryption due to the encryption property inheritance.

To activate filename encryption globally, go to **Settings** and check **Enable filename encryption**.

To change the filename encryption settings of already encrypted items, ctrl-click them and select **Encrypt filename** in the context menu.

How to Decrypt Files

> You do **not** need to decrypt your files when working with Boxcryptor.

If there is a scenario in which you want to decrypt a file, here are some possibilities:

- If you want the decrypted files synced to your cloud provider, the easiest way is to ctrl-click on the file or folder you want to decrypt and select **Create Decrypted Copy**.
- If you want to copy or move your files to another location in decrypted mode, just select the files in the Boxcryptor location within the Finder and copy or move them to the new location. The data will be decrypted automatically.

On-Demand Files

The Finder has a built in On-Demand File feature, what means not all files are automatically synced to your device. Instead, only the directory structure is replicated on your device and files are downloaded on demand when you open or download them (**ctrl-clicking -> "Download Now"**). This saves valuable disk space and bandwidth while still being able to access every file from your computer. If you later decide that you no longer want the file locally, you can simply remove it with **ctrl-clicking -> "Remove Download"**. When you browse into a folder the files will get synchronized.

Share Access to Files

One of the main reasons to use cloud storage is how easy it is to share files and that one can simplify remote group work. Boxcryptor allows you to stay secure while collaborating and sharing files with others.

What You Need to Know About Sharing Encrypted Files

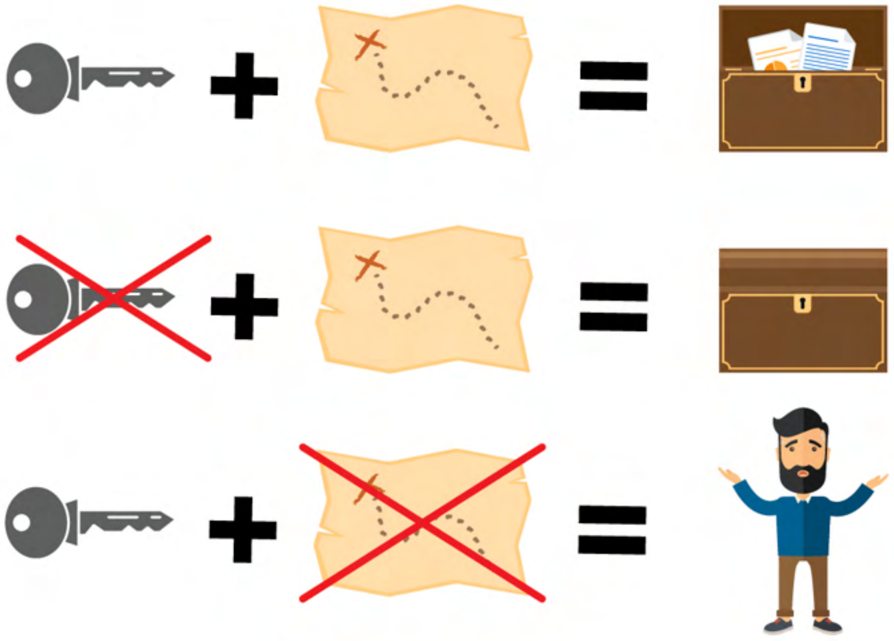
For understanding how the sharing of encrypted files works, it is helpful to understand how programs handle unencrypted and encrypted files.

If you store an unencrypted file on your device or in the cloud, the program you store it with saves the file and the information inside. Such a file can be read or modified by anyone who has physical access. If you encrypt a file, however, the information inside the file is modified. For programs and humans the encrypted information is rendered useless. To decrypt the information again, you need a **cryptographic key** that translates the information back into its original state.

Therefore, **sharing an encrypted file** with somebody is like writing an email by poking around on your keyboard. The other person can read the information, but it is useless, since **it does not have any semantic meaning**.

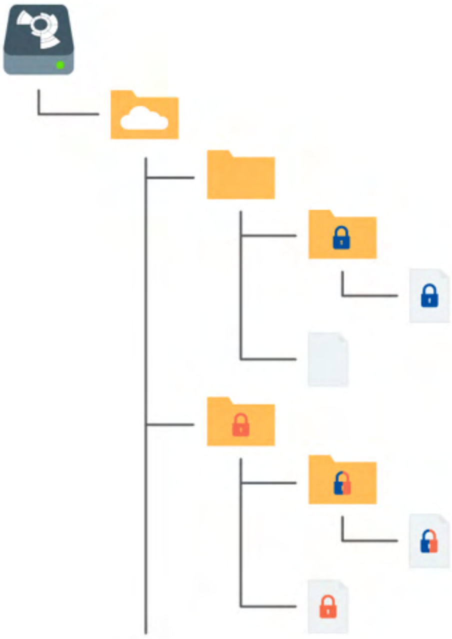
As a consequence, there are two steps necessary to share an encrypted file:

1. Share the file physically at your cloud provider. Please check your provider's documentation on how to share files or folders with others.
2. Share the cryptographic key in Boxcryptor. Boxcryptor uses a key for each file. The key is encrypted by your Boxcryptor account and is stored **within the file itself**. If you share the file with somebody, the key will be encrypted with the Boxcryptor account of the receiver and stored in the file as well.



Note: Every time you share a file, the file is modified. Keep in mind that it must be synchronized by your cloud provider. If you share access to multiple files, make sure that they are all synchronized completely.

Just as the inheritance of encryption properties, permissions are inherited from the parent folder as well. If you add a file to a shared folder, the persons who you shared the folder with can access the file now, too.



🔒 **Encrypted** and **permission to access** for **Alice**

🔒 **Encrypted** and **permission to access** for **Bob**

🔒 **Encrypted** and **permission to access** for **Alice and Bob**

Share Files With Boxcryptor Users: Permissions

If you want to share a file or folder with someone who uses Boxcryptor as well, follow these steps:

- Ctrl-click the **file or folder** → **Manage Permissions**.
- Add the group or user you want to share the file or folder with.
- Apply the changes.
- Wait for the data to be synced to your cloud.
- Make sure to also share access to your file or folder on **your providers web interface**.

> ℹ If you have filename encryption activated, it is considered best practice to create a parent folder without filename encryption and share this folder physically at your cloud provider.

Sharing Data With Non-Boxcryptor Users: Whisply

If you want to share a file with someone who is neither using Boxcryptor nor the cloud, you can use Whisply. Whisply is a browser based secure file transfer service that we developed for this purpose. Please follow the guide of Boxcryptor and Whisply here.

Manage Groups

Groups are a powerful instrument for managing your users and their access rights. Manage your groups in your account when you sign in on our website here.

> ℹ Please be aware that the group feature is only availabe with Boxcryptor Business and up.

Irreversible operations, such as **rename**, **delete**, or **grant** and **revoke ownership** are restricted to the **owner** of the group. You can set other members as owners and also remove ownership. Groups can have multiple owners.

Benefits of Groups

Besides sharing files with individual accounts, you can also **share files with a group of users**. If you share a file with a group, the cryptographic key will be encrypted with a group key and stored inside the file.

The benefits of groups are:

- **Central management**: You do not need to click through all your files to see, revoke, or grant access to somebody.
- **No synchronization necessary**: When you add or remove someone from a group, the changes are done on your machine and our servers only. Therefore it is much faster. Since the permissions within the files do not change, a consecutive file synchronization is not necessary.

Settings

App Protection

In Boxcryptor for macOS, App Protection was replaced by **Files Protection**. Files Protection prevents unauthorized access to **files and folders saved to the Boxcryptor location** within Finder. To use this feature, activate the “Files Protection” switch in your Boxcryptor app and set your personal, six-digit **Boxcryptor passcode**. The passcode is **independent from your device code and Boxcryptor password**.

You can now protect your files and folders by clicking **Home** -> **Lock** in the Boxcryptor-App. This will completely remove your locations from Finder until you unlock again.

Further Setting Options:

- **Touch ID (optional):** In addition to the Boxcryptor passcode, biometric authentication can be used if available on your device.
- **Change Passcode:** For subsequent adaptation of the Boxcryptor passcode.

> To change the settings of the Files Protection in the Boxcryptor app, you always have to re-enter the six-digit Boxcryptor passcode.

> After ten unsuccessful unlock attempts, the Boxcryptor app completely blocks access to your files and folders. To access the data again, you must sign out in the Boxcryptor app itself and sign in again with your email address and your Boxcryptor password.

Note: If a sophisticated attacker gains access to your operating system, it is theoretically possible for him to circumvent the protection feature by directly accessing the applications internal data. While this feature can help you better protect your encrypted data on your computer, it does not guarantee 100% security against sophisticated attackers with access to your operating system. We recommend to follow local device security best practices, to avoid such a situation.

Boxcryptor Settings

Boxcryptor is seamlessly integrated into Apple's **Finder**, so the experience depends heavily on its functions and preferences. However, some settings are only available within the Boxcryptor app.

To get there, open the **Boxcryptor app** and navigate to **Settings**. Here you will find options to:

- enable Filename Encryption,
- autostart Boxcryptor,
- set up the Files Protection,
- and **Sign Out** of your Boxcryptor account to reset the app to factory defaults.

Finder Documentation

To read more about how to work with Finder, have a look at Apple's own documentation.

Boxcryptor Account

Manage Your Account

You can manage your Boxcryptor account by signing in on our website. If you want to change your personal information, such as your first name, last name, email address, or your password, go to the **My Account** page.

Restoring Your Password

Since we offer a zero knowledge service, **we CANNOT reset or tell you your password**, in case you forgot your password. However, we can offer you to completely reset your account.

> ⚠ If you reset your account, new encryption keys will be generated for your account. This means you will irrevocably lose access to **all** your already encrypted files and you will be removed from all groups.

You can reset your account here.

Manage Your Devices and Sessions

Boxcryptor keeps track of all devices and web session connected to your account. A device is created every time you sign in to the Boxcryptor application. A web session is created every time you sign in on our website.

On the devices overview page you can view and unlink your connected devices and web sessions. This is useful, for example, when your device has been lost or stolen and you want to revoke access to your data. Boxcryptor will automatically reset to factory settings on an internet-connected device which has been unlinked.

Note: In the free version, you can only use two devices with your account. If you, for example, get a new mobile phone and want to use Boxcryptor with it, you need to sign out on your old mobile phone, unlink it on the devices overview page or upgrade your account here.

Export Your Keys

It is possible to export your keys, which are stored on our servers, into a local key file. This key file can be used in combination with a local account, which does not require any connection to our servers. Even if our service would be interrupted for a long time or completely shut down, you would always be able to use Boxcryptor to access your files which have been encrypted.

You can export your keys when you sign in to your account on our website:

1. Navigate to **My Account**.
2. Scroll down to the **Advanced** section and click on **Export keys**.
3. You can use your keys as a local account with Boxcryptor.

Exporting your keys is not necessary for using Boxcryptor offline. If you have already been signed into your Boxcryptor account, you can use Boxcryptor offline without any problems. Your keys are already synced to your device.

Local Account

The local account's purpose is to serve as a backup way to your files even if the Boxcryptor servers are not reachable. It achieves this by managing your keys locally in your own key file.

A local account comes with **major restrictions**:

- It is not possible to grant others access to files.
- It is more difficult to switch devices.
- Managing groups is not possible.
- Managing devices is not possible.
- Most features of the Company Package are not available.

We do not recommend the use of a local account on a daily basis. The main purpose is to have a backup of your keys.

How to export a Key File

To use a local account, you will first have to export your keys as described here.

How to Open an Existing Key File

Version 2 (Default)

1. Start Boxcryptor.
2. Click on the **three dots** in the upper right corner of the Sign In window.
3. Choose **Local account**.
4. Choose **I want to use a local account**.
5. Select your existing key file.
6. Enter your password to sign in.

Version 3 (File Provider)

1. Double-click your key file to open it with Boxcryptor.
2. Enter your password to sign in.

Where Can I Delete my Account

If you do not want to use Boxcryptor anymore, you can delete your account. All your information, including your keys, will be deleted permanently from our servers. **Make sure that all your files are decrypted** before you proceed. After the account is deleted, it is **not possible to restore any data**.

ⓘ We recommend performing a key export before. This allows overlooked encrypted files to be decrypted at any time, even after account deletion.

You can delete your account when you sign in here.

Refer-A-Friend

Invite your friends to Boxcryptor and do yourself and your friends a favor. For each successful referral you and your friend will get one month of **Boxcryptor Unlimited for free**. Both, free and Boxcryptor Unlimited users, can take part in the referral program. Free users get their free months immediately and paid users receive extra months which will be added at the end of their running subscription (renewal and payment will be due one month later). You can find your **personal referal link** when you sign in to boxcryptor.com.

In order to qualify for a successful referral, your friend has to verify his or her account, and sign in once. The sign in must occur in one of our installable desktop apps on a separate device.

Once a friend has joined Boxcryptor via your referral link, it will show up in your overview in the web interface. A referral can have the following statuses:

- **Waiting for verification**: Your friend did not yet verify the account. To do so, the referred person must click on the verification link sent to his or her email address.
- **Waiting for sign in**: Your friend did not yet sign into the account in one of our desktop apps on a separate device. Signing in on a device which has already been used for another referral will not work.
- **Waiting for account change**: You cannot claim the bonus because you are a company user. Only regular Free or Unlimited users can claim referral bonuses.
- **Earned**: Your friend completed all steps required so that you can claim your bonus. Click the link in order to claim it.
- **Claimed**: You have claimed and received the bonus for the referral.

Two-Factor Authentication

Two-Factor Authentication (2FA) will require you to proof your identity with a second factor during the sign in. This second factor is generally something that the user posesses, such as a physical, second device. The advantage of this procedure is that when an attacker gets hold of (or guesses) your password, he still needs access to your physical device - so you're still safe. Boxcryptor is offering 2FA using authenticator apps or security keys.

Authenticator App

Authenticator apps use the Time-based One-Time Password algorithm (TOTP) to generate secure 6-digit code on your mobile device which have to be entered during authentication. To use it, **you need to install an Authenticator App** of your choice on your mobile device. Next, you need to configure both your Boxcryptor account and your authenticator app using the following steps:

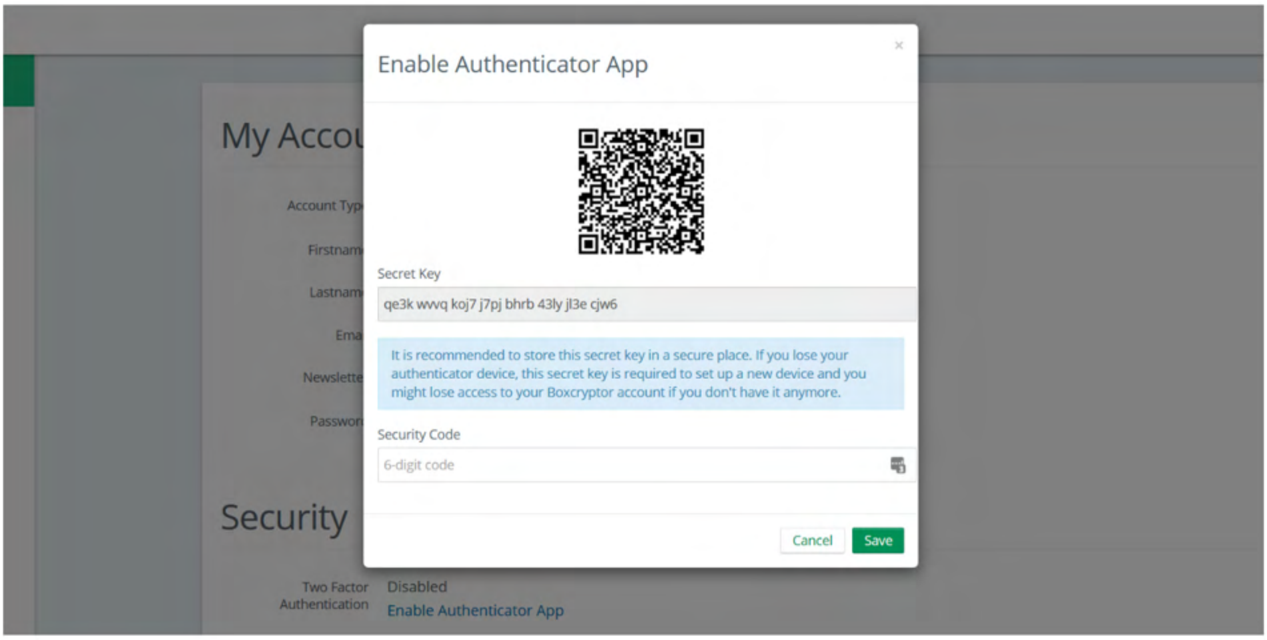
1. Sign in to boxcryptor.com.

2. Navigate to **Security**.
3. Click on **Two-factor Authentication -> Authenticator App**.
4. Scan the QR code with your Authenticator App. Copy the **Secret Key** and store it in a secure place.
5. To complete the setup, enter the 6-digit code from your authenticator app.

From now on, you will need to provide both your credentials and a 6-digit code from your authenticator app to sign in. Since the code is time-based, it will change all 30 seconds.

Read more about authenticator apps in our blog.

Important: In case of losing your second device, you can use the secret key to configure a new authenticator app on another device. Afterwards, you can use this device to sign in to your account again. In this case, we recommend changing the authenticator app as a next step, to ensure that the lost device can no longer be used for sign ins. Please store your secret key wisely. It looks similar to this:



Enable Authenticator App

Secret Key

qe3k wvvq koj7 j7pj bhrb 43ly jl3e cjw6

It is recommended to store this secret key in a secure place. If you lose your authenticator device, this secret key is required to set up a new device and you might lose access to your Boxcryptor account if you don't have it anymore.

Security Code

6-digit code

Security

Two Factor Authentication: Disabled

Enable Authenticator App

It's possible that backups of the mobile device and the subsequent recovery will cause settings (pages) in the authenticator app to be lost. We therefore recommend to make a separate backup of the settings beforehand (for example, by backing up the secret keys or using in-app backups). Alternatively, you can setup a security key as a second factor backup.

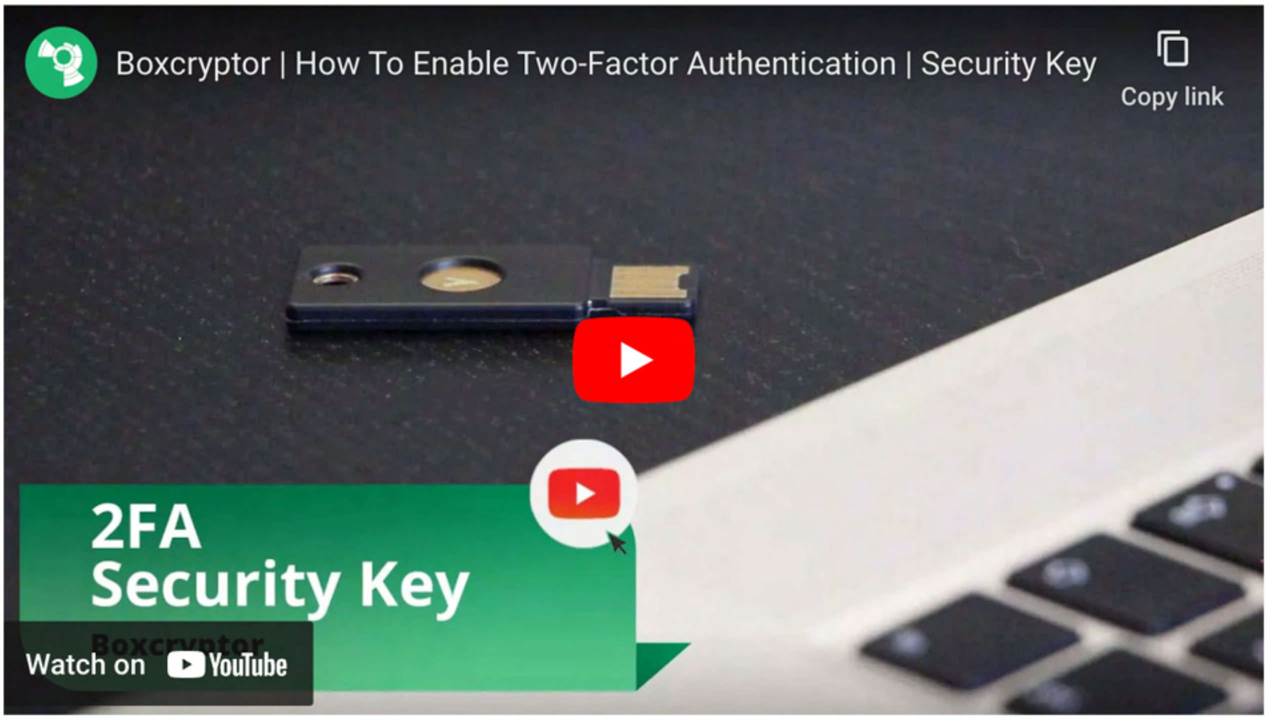
Security Keys

Security keys use the WebAuthN protocol to prove your identity by a simple tap on the device. To use this feature, you need a security key. Next, you need to configure your Boxcryptor account using the following steps:

1. Sign in to boxcryptor.com.
2. Navigate to **Security**.
3. Click on **Two-factor Authentication -> Security Keys**.
4. Select **Add Security Key** and follow the instructions on the screen.

From now on, you will need to provide both your credentials and a verification with your security key to sign in.

Read more about security tokens on our blog


Boxcryptor | How To Enable Two-Factor Authentication | Security Key
Copy link
2FA
Security Key
Boxcryptor
Watch on YouTube

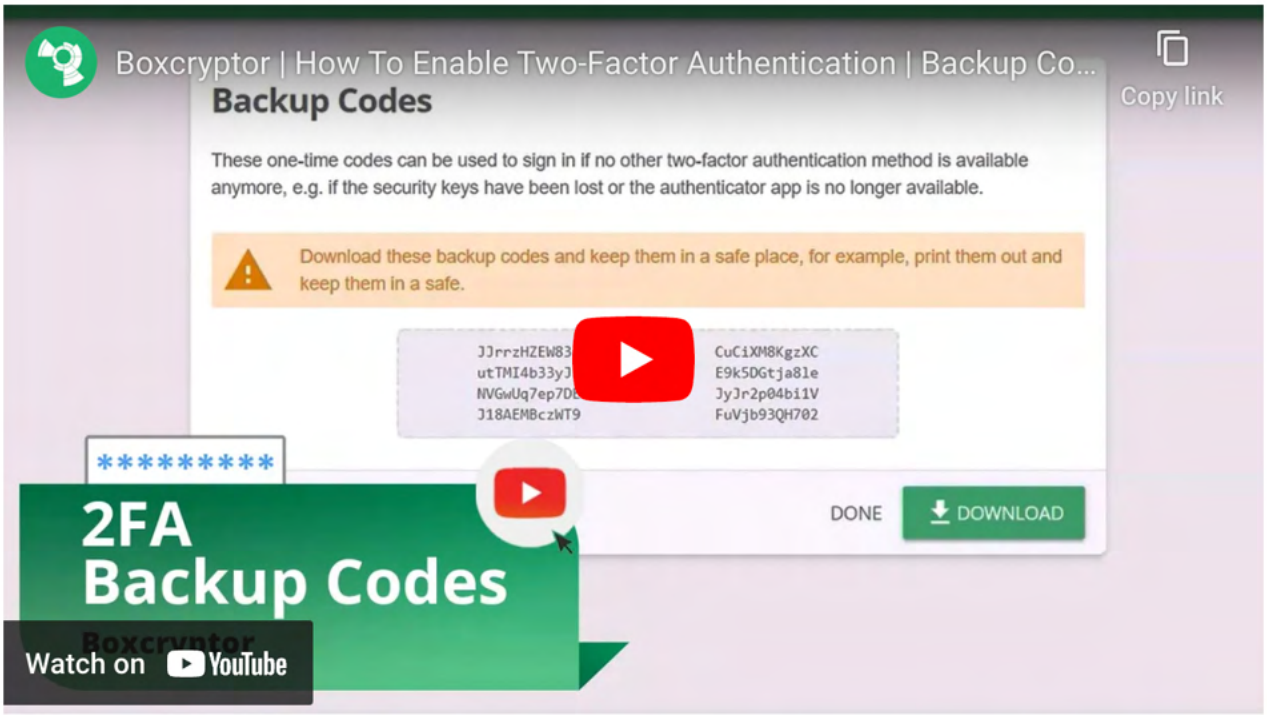
To prevent a lockout we recommend registering two security keys. Use one regularly, keep the other one as backup in case that you loose the first one. Alternatively, you can set up TOTP as a second factor backup.

Limitations: Security keys are currently **not** supported on Boxcryptor for iOS, Boxcryptor for Android and Boxcryptor Portable. In these cases, you won't be able to sign in if 2FA is enabled. If accessing your account over boxcryptor.com, you need to use a modern browser.

Backup Codes

Backup codes are one-time codes that can be used as an alternative to the second factor, if e.g. the security key has been lost or the mobile phone with the authenticator app is not available. To add backup codes to your account, you need to configure your Boxcryptor account using the following steps:

1. Sign in to boxcryptor.com.
2. Navigate to **Security**.
3. Click on **Two-factor Authentication -> Backup Codes**. (This option only is visible when at least one second factor was added to the account.)
4. Now the newly generated backup codes are displayed at the screen.



Boxcryptor | How To Enable Two-Factor Authentication | Backup Co...
Copy link

Backup Codes

These one-time codes can be used to sign in if no other two-factor authentication method is available anymore, e.g. if the security keys have been lost or the authenticator app is no longer available.

Download these backup codes and keep them in a safe place, for example, print them out and keep them in a safe.

```
JJrrzHZEW83        CuCiXM8KgzXC
utTMI4b33yJ        E9k5DGtja8le
NVGwUq7ep7DE       JyJr2p04bi1V
J18AEMBczWT9       FuVjb93QH702
```

We recommend downloading the backup codes and keeping them safe. In order to benefit from the backup codes, you need to have the codes available when you are logged out.

2FA and the Protection feature

2FA is only enforced when signing in to your Boxcryptor account. Once you are signed in, the second factor is not required anymore - even if you enabled the Protection feature. The Protection feature helps you to prevent unauthorized access to Boxcryptor when you're **already** signed in and you won't be asked for your second factor. To make Boxcryptor ask you for your second factor, you first need to sign out completely.

Limitations: Boxcryptor for Chrome (beta) do **not** support 2FA. That means, you will be not able to sign in, as long 2FA is enabled. However, the following workaround exists:

1. Go to boxcryptor.com and disable 2FA.
2. Sign-in in the Boxcryptor client.
3. Enable 2FA again.

FAQ & Troubleshooting

Off-Migration Guide: Decrypt all Boxcryptor encrypted files

With Dropbox acquiring several key assets from Secomba GmbH i.L., Boxcryptor will be discontinued and we will cease our service. All users and customers will be able to continue using the service until the end of their contractual term.

To migrate away from Boxcryptor, you will have to decrypt all your files to keep access to them.

> If you are concerned that you might lose access to files encrypted by Boxcryptor you currently do not have physical access, we strongly recommend downloading the latest client software and **exporting your keys** as described here.
> This way, even after your account has been deleted or the Boxcryptor service is shut down, you will be able to decrypt any files later on.

Migration Tips For Organizations

- Administrators are able to export the keys of all users by clicking on each user and selecting `EXPORT KEYS` in the User Management.
- Self-service key export for users is **not allowed** by default. This restriction can be lifted by enabling the `Allow Key Export` policy here.
- If **Master Key** is enabled, the key export of an administrator account will include **all keys of all users with an active Master Key**. This enables overall access to all of the organization's files.

Decrypting your files is easy: You can simply copy and paste all files within the Boxcryptor drive to a secure location using `CMD+C` on the source files and `CMD+V` in the target directory. Alternatively, you can use the Finder's context menu entries for that.

When everything is decrypted, you can then delete all encrypted source files.

> If you have many files to migrate and would run into low disk space issues doing so, you might want to decrypt and delete the corresponding source files in batches.

What happens if Boxcryptor goes out of business?

Boxcryptor has been designed in such a way that Boxcryptor continues to work even if the Boxcryptor servers are not available and you're still signed into Boxcryptor. If you want to take additional precautions for the event that the Boxcryptor servers would go permanently offline, you must have the following backups:

- Exported key file
- Boxcryptor installer file

When these files are available, you will always be able to access your encrypted files on your own on any supported operating system - without any connection to any server. The exported key file contains all encryption keys associated with your Boxcryptor account. *Important:* As new keys might be added over time by Boxcryptor's integrated key management (e.g. when sharing files with other Boxcryptor users), it is recommended to regularly export a new key file.

After installing Boxcryptor, you can use the exported key file to access your encrypted files using a local account. Learn more about exporting your keys and local accounts.

Migrate to Boxcryptor for macOS v3.x

With the use of Apple's File Provider framework introduced in **macOS 12**, we can finally provide an **all-new Boxcryptor for macOS app** that seamlessly integrates into Apple's Mac ecosystem, similar to Boxcryptor for iOS app.

System requirements

Boxcryptor for macOS v3.x supports **macOS 12.0** and later.

1. Preparation - FileVault

With Boxcryptor, files stored in the cloud are always encrypted and encryption is performed locally on your Mac all the time. **Only encrypted files leave your device.**

However, in contrast to Boxcryptor for macOS v2.x, **files stored locally on your Mac are not encrypted** by Boxcryptor anymore due to technical limitations by Apple's File Provider platform. File Provider apps must store files in clear text on the local file system so that their content can get picked up by macOS and presented to the user. This affects file contents and file names.

Here's the encryption state by location:

- **In the cloud:** Files are always protected by Boxcryptor's encryption
- **On your Mac with FileVault:** Files are protected by FileVault's encryption
- **On your Mac without FileVault:** Files are not protected (not recommended)

We strongly recommend the use of local full-disk encryption for every Mac – regardless if you are using Boxcryptor for macOS v2.x or the new v3.x, or even if you don't use Boxcryptor at all. Full-disk encryption is an integral part of local device security and can easily be achieved by turning on FileVault on any Mac.

> ⓘ By using FileVault, files available in Boxcryptor for macOS v3.x are still protected by FileVault's encryption on the local disk, despite appearing as clear text when your Mac is in use. Learn more about FileVault here: https://support.apple.com/en-us/HT204837

2. Installation

Boxcryptor for macOS v3.x is a native File Provider app which works "out-of-the-box" on modern macOS operating systems. Additionally, the app is now fully utilizing the macOS sandboxing security mechanism. All you need to do is download the latest version and follow the standard installation process.

3. Add Clouds and Locations

Boxcryptor for macOS v3.x **includes the full functionality for fast, smooth and secure synchronization of your files and folders.** To make use of this, directly connect your cloud provider to the app by the following steps:

1. Navigate to the **Home** tab
2. Click **Add Provider...**
3. Select your desired Service
4. Authenticate with the credentials of your cloud provider

> Your credentials are sent directly to the service you choose, they are **not** sent to our servers.

If you don't want Boxcryptor to sync your files itself, you can still work with your installed sync clients. To do this, select **Local Storage** in your Boxcryptor app and choose the sync folder of your provider's client.

> As every File Provider app, Boxcryptor is now available in `~/Library/CloudStorage` where a sync folder for each connected cloud provider is created. These folders are also accessible in the **Finder's Location section.**

4. Remove Boxcryptor for macOS v2.x

Since Boxcryptor for macOS v2.x is deeply integrated into macOS and the system does not provide an uninstall mechanism by default, follow these instructions to completely remove the app from your system:

1. Quit Boxcryptor
2. Open **System Preferences** → **Extensions** → **Finder Extensions** and disable Boxcryptor
3. Delete the following folders:

- ~/Library/Application Support/Boxcryptor
- ~/Library/Logs/Boxcryptor
- Volumes/Secomba

> The **~/Library** denotes the **user library** folder and NOT the **system library** folder.

4. Remove application preferences by executing the following command in the **Terminal** app: *defaults remove com.boxcryptor.osx*
5. Open the **Keychain Access** app and remove all entries starting with com.boxcryptor.osx
6. Move **Boxcryptor.app** into trash

5. Reset Security Policy

If you changed your Mac's Security Policy to Reduced Security due to Boxcryptor for macOS v2.x, you can then revert this policy back to **Full Security** by following these steps:

1. Reboot your Mac into Recovery Mode
2. Open Utilities → Startup Security Utility
3. Select and unlock your system volume and click Security Policy...
4. Choose Full Security
5. Restart your Mac

6. Remove Sync Clients

In addition, Boxcryptor for macOS v3.x is all you require installed on your Mac to work with encrypted files in Dropbox, OneDrive, Google Drive or any other supported cloud provider. You can now remove your cloud provider's client from your Mac.

Further information

File name and type restrictions

Due to technical reasons, the following file types cannot be stored in Boxcryptor:

- App Bundles (.app)
- Frameworks (.framework)
- XIP (.xip)
- Crash Files (.xccrashpoint)
- Boxcryptor Files (.bc, .bch, .bclink)
- Apple Archive Files (.abbu, .icbu)

If required, this file type restriction can be bypassed by zipping the files.

Additionally, file name or type restrictions by used cloud providers apply.

Spotlight

A major advantage of the new File Provider-API over the old virtual drive is that Spotlight works out-of-the-box without requiring special handling by Boxcryptor. This means that **Spotlight indexes visited files and folders in Boxcryptor locations automatically and by default.** Spotlight support is not an optional advanced setting anymore, but a first-class default experience for every user.

Spotlight indexes file and folder metadata of all items in Boxcryptor locations. File contents are only searchable for downloaded files which are locally available for indexing due to technical limitations.

Why is everything new?

A main driver for the new Boxcryptor for macOS version is Apple's strategy to disallow third-party kernel extensions on macOS to further secure and close down the Mac operating system. Apple started to deprecate third-party kernel extensions a few years ago and successively made it more difficult to use them. While a kernel extension could be loaded "on-the-fly" in the past, macOS 10.15 Catalina started to require a system reboot during the loading process.

Nowadays, Macs with Apple Silicon processors additionally require the modification of the Mac's Security Policy in Recovery Mode to allow third-party kernel extension loading. All signs indicate that third-party kernel extensions will not work at all in future versions of macOS. Holding on to our existing concept using a virtual Boxcryptor drive based on a kernel extension would not be sustainable anymore.

Due to Apple's decisions, we have been forced to come up with a new concept how Boxcryptor for macOS works in the years to come. At the same time, we are excited about the new possibilities and experiences this new integration into macOS opens up for Boxcryptor in the future.

Documentation for Boxcryptor 2.x (Legacy)

This documentation covers our new Boxcryptor for macOS app that requires **macOS >= 12**. If you need assistance to our old Boxcryptor app, you can download the legacy documentation here.

How to Create a Debug Log

What is a Debug Log?

A debug log captures all internal events while Boxcryptor is running. It can help us to track down issues with Boxcryptor, for example bugs and incompatibilities with other software.

Does a Debug Log Contain Sensitive Data?

When you create a debug log, sensitive user information - like password, encryption keys, or actual file content will **not** be logged.

Which Information Does a Debug Log Contain?

The debug log captures the following information.

- User interaction such as button clicks and in-app navigation
- File operations (**including unencrypted filenames**)
- Current Boxcryptor settings
- Communication with our servers and your cloud provider(s)
- System information such as OS version or required frameworks
- Running programs

How Do I Create a Debug Log?

1. Open the **Console** app.
2. Enter `com.boxcryptor.` into the top right search bar and press **Enter**.
3. Click **Start**.
4. Reproduce the issue you have with Boxcryptor for macOS (if you have synchronization issues, please give it some time to hypothetically finish).
5. Switch back to the **Console** app.
6. Click **Pause**.
7. Select and copy all log entries using **CMD+A** and **CMD+C**.
8. Open **TextEdit** (or any other text editor of your choice).
9. Paste the log entries using **CMD+V**.
10. Save the file as **boxcryptor.log**.

What Should I Do With my Debug Information?

Use our Boxcryptor help form to **send us the file with a detailed description of the problem** or write to our support team, with the attached debug information.

I Cannot Connect to the Boxcryptor Servers

Depending on your system or network configuration, Boxcryptor may not always be able to communicate with our servers. However, there are some workarounds for the following scenarios.

Error Message like “No Connection” or “Sync Keys failed”:

When this error message shows, make sure that you still have internet access with Safari. Make sure that the Boxcryptor server status here returns the message **OK**. One possible source of error could be your proxy settings. For example, try adding `api.boxcryptor.com` to an exclusion list.

Warning: This is no Secure Connection

If you are in an environment that performs **traffic inspection**, you might not be able to connect to our servers. Examples, where traffic inspection might interfere with Boxcryptor:

- Anti-virus solutions that protect internet traffic
- Public hotspots
- Company proxy servers
- **Malware**

Traffic inspection, techically speaking, is a **man-in-the-middle attack**. Therefore, it is important to make sure your system or internet connection is not compromised. You can check the certificate information provided, by clicking **advanced** in the error message.

Working Offline

If you already have signed in to Boxcryptor sucessfully, you can continue to work on your already opened or downloaded files offline. However, you will not be able to alter Boxcryptor permissions or use other online features of Boxcryptor.

Use self-signed Certificates for Cloud Provider

Connecting to self hosted WebDAV or Owncloud / NextCloud instances with **self-signed certificates** does not always work out-of-the-box.

For Boxcryptor to connect to your server, you must install your self-signed certificate on your device. For more information how to install it, please see here.

For more information on certificate requirements, check apple's specification here.

ℹ If you own the domain, you can instead create a **free and trusted certificate**. For more information, see Authorities such as **Let's Encrypt**.

I Cannot Move a File to an Encrypted Folder

Moving files between differently encrypted folders or into a new encrypted folder always requires encrypting the files with the new folder key. Hence, Boxcryptor has to download the item, decrypt, encrypt, and upload the item again. Due to the complexity, we decided to disable the option to move and copy between encrypted folders.

ℹ Alternatively, you can simply **copy** files to the desired folder and finally delete the original items.

Where can I download Boxcryptor Classic?

Boxcryptor Classic is the predecessor of Boxcryptor which has been discontinued. It is not recommended to use Boxcryptor Classic because it is not supported anymore and does not work on the latest operating system versions.

If you're an existing user of Boxcryptor Classic you can download it here and we recommend you to upgrade to Boxcryptor as soon as possible.

Download Boxcryptor Classic for Mac OS X here:
https://www.boxcryptor.com/download/Boxcryptor_Classic_v1.5.415.252_Installer.dmg *Supports Mac OS X 10.7, 10.8, 10.9, 10.10*

If you already upgraded to Mac OS X >= 10.11 and need to decrypt your encrypted files with Boxcryptor Classic, you can download this “unofficial” version with read-only support for macOS 10.11 and 10.12:
https://www.dropbox.com/s/wbrygn4x2kgzlsp/Boxcryptor_Classic_v1.5.417.253_Installer.dmg?dl=0

Outdated Clients

We regularly release new versions of Boxcryptor with new features, better stability and overall improvements and retire outdated versions over time. On **September 30 2018**, the following versions have been retired:

- Boxcryptor for **Windows 2.22.706** and older
- Boxcryptor for **macOS 2.19.907** and older

When you try to use a retired version, you will not be able to use Boxcryptor and receive one of the following error messages:

> This client is invalid or outdated. Please upgrade to the latest version.

> The client id is invalid!

> This is no secure connection

> The remote certificate is invalid according to the validation procedure

---

> Boxcryptor can't establish a secure connection to the Boxcryptor server.

Solution

Download and install the latest version of Boxcryptor from here. Afterwards you will be able to continue to use Boxcryptor.

ℹ If you still see the error message **This is no secure connection**, the problem lies elsewhere. Check out **I Cannot Connect to the Boxcryptor Servers**.

I am using Windows XP or Mac OS X 10.14 or earlier

Current versions of Boxcryptor require Windows 7 and later or macOS 10.15 and later. As all earlier operating system versions are not supported by Apple or Microsoft anymore, we recommend affected users to update their operating system to a newer version as soon as possible in order to stay safe.

Using unsupported operation systems poses a huge security risk. You really have to update your operating system for security-related use.

I cannot update to the latest version

Note: If you are using **Windows**, please look into I Cannot Update or Uninstall Boxcryptor first.

If for any reason you cannot update to the latest version and can't access your encrypted files anymore, you have the following options:

Boxcryptor Portable

Boxcryptor Portable does not require any installation and can be used to access and decrypt your encrypted files without administrator rights. Download Boxcryptor Portable here.

Key Export

You can export your keys from our server and use a local account to sign in to your outdated Boxcryptor version without requiring a connection to our servers. Learn more here.

I cannot sign in due to too many connected devices

Sign in to your account at boxcryptor.com and remove a device which is no longer needed. Then try again to sign in.

Cannot open some files

There may be situations where files appear to be inaccessible. This can have multiple reasons:

Boxcryptor Access Issues

> On desktop some Applications or the file browser shows a message with `Invalid parameter` when trying to open a file.

- Boxcryptor is eventually signed-in to a wrong account. → Check the account info in the Boxcryptor settings and compare it with the Boxcryptor permissions.
- The user has no Boxcryptor permissions on the file. → Make sure the user has physical access to the shared file, has *Boxcryptor permissions* correctly set and the latest permission changes of the file have been *synced*. Learn how to set permissions here.

Filesystem Permissions Issues

> Files are *read-only* or "permission denied" is displayed. Change files system permissions so your user can (physically) access them.

Sync Issues

> "Bad padding" issues, empty physical files or inaccessible folders due to an empty `Folderkey.bch` file.

> File open shows "Found invalid data while decoding" and the .bc file is empty.

> Folder cannot be opened "Found invalid data while decoding." is displayed in the permission settings.

There has been an incompatibility with Dropbox in the past that could create "broken" content for smaller files because Dropbox did not sync the last file change.

- restore an older version of the corrupted file via the file history of your cloud storage provider.
- for folder issues, delete the empty `Folderkey.bch` file and *re-encrypt* the folder.

Apple Chip-Support

On November 10, 2020, Apple revealed new Mac hardware with the revolutionary Apple Silicon M1 processors which are available since November 17. Boxcryptor has been adapted to run natively on the new processor architecture with the maximum performance and battery life.

Boxcryptor natively supports the new Apple Silicon Macs since version 2.39.1119 released on December 18, 2020.

What is a FolderKey.bch and a .bclink file

There is a File Called FolderKey.bch in my Cloud Storage. What is This?

Boxcryptor creates a **FolderKey.bch** file when a folder is encrypted. It contains encryption metadata for its parent folder and helps Boxcryptor to maintain the encryption hierarchy. This file is not visible within the Boxcryptor drive.

Does it Leak Sensitive Information?

The FolderKey.bch does not contain any sensitive information. Only .bc files contain sensitive information — and these are encrypted.

What Happens When I Lose it?

Dont't worry, you will not loose any data or access to files. All crypto-required information is stored directly within your encrypted *.bc files.

The downside of losing that file is that Boxcryptor no longer perceives the parent folder as encrypted. As a consequence, new files in this folder will not inherit the encryption setting.

There is a File Called .bclink in my Cloud Storage. What is This?

The file helps to verify the account when linking accounts to use features like Whisply.

If the file doesn't exist, the user either used a different account for linking or the sync client is not turned on/syncing.

Does it Leak Sensitive Information? Can I delete it?

The file does not contain any sensitive information. It is not necessary and can also be deleted. However, it may be generated again automatically.

Recover Account Access if Second Factor (2FA) is Lost

In the case of a lost second factor for the two-factor authentication (2FA) such as an **authenticator app**, your mobile device in total, your **security key** or other hardware, you will no longer be able to sign in to your Boxcryptor account.

Ways to recover access to your account:

Re-apply the secret key from your initial setup

If you still have your secret key from the initial Authenticator App setup, you can just re-add it to your authenticator app of choice. Next to the QR Code scan method these apps usually provide a "manual" way to add a Time-based One-time Password (TOTP) account.

For reference, the secret key looks similar to:

> mzwe wocd mj3d qr3f njjw g2cm grqw cvli

Use a device code

If you are still recently signed-in in **Boxcryptor for Windows** or **Boxcryptor for macOS**, You can use these devices as a second factor instead.

The second factor authentication screen will then provide you with the extra option "Use Device Code". Upon clicking on it, our apps will provide you with a temporary 8-digit pin, that will be valid for 5 minutes.

Please ensure that your Boxcryptor client is up-to-date before. You can always download the latest version here.
Also, make sure the Boxcryptor client is started and **unlocked** before requesting a device code.

Use a backup code

Once you set up your second factor, **backup codes** will be generated and presented to you. You can use these **one-time** codes instead of your second factor.

If you run out of one-time codes, you can regenerate new codes here.

None of the above methods apply

If you are still unable to access your account, you can also contact us to disable the two-factor authentication.

However, we need clear evidence that you are the legitimate owner of this account.

The identification will be done via video live chat, you will need the following things:

1. A device with a **browser** installed and a **working camera**.
2. An **identification** of your **person** (ID card, passport or driver's license).
3. The **valid e-mail address** of your **Boxcryptor account**.

To pick an appointment, please visit our **Booking Page**.

Please provide a valid e-mail address, since it will be used for a calendar invite, further instructions and a meeting join link.

As a video chat platform, we use **Microsoft Teams**. You **do not need a user account** there. On desktop computers, a modern browser (Chrome, Edge or Safari) is sufficient. For other browsers or mobile devices, you might have to download the Microsoft Teams App:

iPhone & iPad: https://apps.apple.com/app/microsoft-teams/id1113153706 Android: https://play.google.com/store/apps/details?id=com.microsoft.teams Desktop: https://www.microsoft.com/en-us/microsoft-teams/download-app

Invalid Authenticator App Codes

If you are unable to generate a valid code despite the authenticator app working, this is most likely due to a different time on one of the systems involved.

Since these TOTP codes are only valid for 30 seconds, deviations from real time of just a few seconds can lead to registration problems.

You can check the synchronization on all participating devices by visiting the following website: https://time.is

If the time difference is more than a few seconds, we recommend that you set up the automatic time synchronization of your devices or, if necessary, perform a new one.

About

Maintenance Window

In order to constantly improve our service and to keep our servers up-to-date, we regularly maintain our infrastructure. Tasks which might have an impact on the availability of our service will be conducted in weekly maintenance windows at the following time:

Every Monday, 00:00 - 02:00 UTC+1 (4pm - 6pm UTC-7)

We do our best to provide a high availability of our service, but during these two hours access to our servers might be degraded and/or even unavailable. Boxcryptor has been designed in such a manner, that access to our servers is not required for the regular usage of our client software. As outlined in our Technical Overview (chapter *Why and when Boxcryptor requires an internet connection*), only the following actions require an active connection to our servers:

- Creating a Boxcryptor account
- Setting up a new device
- Sharing access to a file or folder
- Account syncing

If you are already signed in with your Boxcryptor account on a device, you are always able to access your encrypted files regardless of your internet connection or availability of our servers.

Changelog

Version 3.12.379 (2022-11-24)

- Improved: Faster encryption and decryption
- Improved: Partially encrypted filenames can be decrypted as well
- Improved: Make all SharePoint Document Libraries accessible
- Improved: Improved warning messages
- Improved: Updated list of non supported file types
- Improved: Dates not available show provider addition date instead of 1677
- Fixed: Several application crashes
- Fixed: Ever-incrementing renames
- Fixed: Encryption required policy not respected
- Fixed: Dropbox "+" signs in filenames get removed
- Fixed: Duplicate files when moving them into folders without permissions
- Fixed: Dropbox shared encrypted filenames could not be renamed
- Minor bug fixes and improvements

Version 3.11.318 (2022-10-17)

- Fixed: Sign in button not working under certain circumstances
- Minor bug fixes and improvements

Version 3.10.314 (2022-10-14)

- Added: Network storage provider
- Improved: Large folder uploads
- Improved: Sign in with local account
- Improved: Better recovery from extension crashes
- Improved: Notification about remote changes when opening Microsoft Office files
- Improved: Local file cache cleanup
- Changed: On deletion, Google Drive files are moved to Google Drive's trash instead of being permanently deleted
- Fixed: OneDrive Personal and Work accounts cannot be added at the same time
- Fixed: Dropbox fails to upload items with plus sign in name
- Fixed: Google Drive files are permanently deleted on removal
- Minor bug fixes and improvements

Version 3.9.264 (2022-09-20)

- Added: Support for .dmg disk image files
- Improved: Better recovery from extension crashes
- Fixed: Handling for various extension errors
- Fixed: Duplicate folders when running into rate limiting while creating large folder structures
- Fixed: Duplicate folder names in Google Drive Shared Drives
- Minor bug fixes and improvements

Version 3.8.254 (2022-09-08)

All new Boxcryptor for macOS. Read more about it in our blog.

Version 2.47.1885 (2022-10-19)

- Added: Compatibility with macOS 13 Ventura
- Added: Support for Google Drive File Provider client

Version 2.46.1667 & 2.46.1668 (2022-03-21)

> This version **is the last with support for macOS Catalina (10.15)** anymore. As this old version is not supported by Apple anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- Added: Mitigation for Dropbox on macOS 12.3
- Fixed: Opening online-only files in OneDrive and Box fails on the first attempt

Version 2.45.1654 & 2.45.1655 (2022-03-14)

- Added: Device code two-factor authentication
- Added: Dropbox incompatibility warnings for macOS 12.3
- Minor bug fixes and improvements

Version 2.44.1601 & 2.44.1602 (2022-01-31)

- Added: Support for OneDrive for Mac v22 with updated Files On-Demand experience
- Added: Support for Box Drive on macOS File Provider Extension mode

- Fixed: Opening PDF files in Adobe Acrobat DC may fail on macOS 12.1
- Changed: Removed path length restriction for Microsoft Excel
- Minor bug fixes and improvements

Version 2.43.1464 & 2.43.1465 (2021-10-14)

- Fixed: Microsoft Teams private channels are not correctly auto-detected
- Fixed: Multiple mirrored Google Drive accounts are not correctly auto-detected
- Changed: Updated BCFS to v4.2.1
- Minor bug fixes and improvements

Version 2.42.1436 & 2.42.1437 (2021-09-20)

> This version has **official support for macOS Monterey (12.0)**.

> This version **does not support macOS Mojave (10.14)** anymore. As this old version is not supported by Apple anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- Added: Support for macOS Monterey 12.0
- Added: Auto-detection for new Google Drive for desktop client
- Changed: Dropped support for macOS Mojave 10.14
- Changed: Updated BCFS to v4.2.0
- Minor bug fixes and improvements

Version 2.41.1307 & 2.41.1308 (2021-05-31)

- Fixed: Cannot sign in if Google Chrome v91 is the default browser
- Minor bug fixes and improvements

Version 2.40.1233 & 2.40.1234 (2021-03-29)

> This version **does not support macOS Sierra (10.12) and macOS High Sierra (10.13)** anymore. As these old versions are not supported by Apple anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- New: Microsoft Teams integration
- Changed: Dropped support for macOS Sierra 10.12 and High Sierra 10.13
- Fixed: Google Drive File Stream v45 is not correctly auto-detected
- Minor bug fixes and improvements

Version 2.39.1119 (2020-12-18)

> This version has **official support for Apple Silicon M1 chips**.

This version only runs on **macOS 11 Big Sur**. For macOS 10.12 Mojave - 10.15 Catalina, use version 2.38.1090.

- Added: Support for Apple Silicon M1 chips
- Changed: Updated BCFS to v4.0.4
- Changed: Updated OpenSSL to v1.1.1i
- Changed: Removed Chromium Embedded Framework
- Minor bug fixes and improvements

Version 2.38.1090 (2020-12-01)

This is the latest version for **macOS Sierra (10.12) and macOS High Sierra (10.13)**.

- Reverted: Used space on the Boxcryptor disk includes purgeable space which is actually freed automatically by macOS if more free space is required

Version 2.38.1086 (2020-11-30)

- Fixed: Google Drive File Stream v44.0.10.0 is not correctly auto-detected
- Fixed: Too many SpiderOak ONE locations are auto-detected. Auto-detection is now restricted to the SpiderOak Hive folder
- Fixed: The Boxcryptor disk freezes under certain circumstances when being mounted
- Fixed: Used space on the Boxcryptor disk includes purgeable space which is actually freed automatically by macOS if more free space is required
- Fixed: Offline mode does not work correctly under certain circumstances
- Fixed: macOS 11.1 is identified as an unsupported macOS version
- Minor bug fixes and improvements

Version 2.37.1043 (2020-11-04)

- Minor bug fixes and improvements

Version 2.36.1042 (2020-10-16)

This version has **official support for macOS Big Sur (11.0)**.

- Added: Support for macOS Big Sur 11.0
- Added: Support for Google Drive shortcuts
- Added: Auto-detection for MagentaCLOUD, CloudMe, SpiderOak, Storegate and Yandex
- Removed: Support for Spotlight (see note below)
- Improved: Compatibility with various backup solutions
- Improved: Symlinks are followed inside the Boxcryptor drive if they target another location
- Changed: Sign out is now part of the account preferences

- - Changed: Updated BCFS to v3.11.2
- Fixed: Administrators could not change permissions to other groups using the Master Key
- Fixed: Local privilege escalation
- Minor bug fixes and improvements

Note: We had to temporarily remove support for Spotlight due to new incompatibilities introduced in past macOS updates and which could not yet be resolved. We are very sorry and do our best to bring it back as soon as possible.

Version 2.35.1024 (2020-06-22)

- Fixed: Documents-based apps (e.g. Office Files like Excel or Word) cannot save documents when the Boxcryptor drive is mounted as fixed drive and the apps are not granted Full Disk Access in macOS 10.15 Catalina privacy preferences
- Fixed: "Bad file descriptor" error when appending data to existing files in certain circumstances.
- Minor bug fixes and improvements

Version 2.34.1023 (2020-06-09)

- Added: Support for file names with Unicode 6
- Added: Disable Whisply policy
- Added: Leitz Cloud and Egnyte auto-detection
- Changed: Enforced password length restrictions for local accounts
- Changed: Updated BCFS to v3.10.5
- Fixed: Files with very long encrypted file names are truncated by iCloud
- Fixed: SharePoint Online auto-detection is broken if the path contains an Umlaut
- Fixed: Strato HiDrive, OwnCloud and NextCloud auto-detection
- Minor bug fixes and improvements

Version 2.33.1015 (2020-02-24)

- Fixed: Sign in is required on each app start when using Single Sign-On
- Changed: Removed SSL Pinning in favor of certificate transparency
- Minor bug fixes and improvements

Version 2.32.1010 (2019-12-16)

- Fixed: Incompatibility with Kaspersky Internet Security
- Changed: Updated BCFS to v3.10.4
- Minor bug fixes and improvements

Version 2.31.1006 (2019-11-07)

- Fixed: Opening OneDrive online-only files fails
- Improved: Mount resilience on broken macOS systems
- Minor bug fixes and improvements

Version 2.30.1004 (2019-10-07)

- Fixed: Crash on macOS 10.12 when removing a location
- Improved: Connection to Microsoft OneDrive

Version 2.29.1001 (2019-09-25)

This version has **official support for macOS Catalina (10.15)**.

This version **does not support Mac OS X El Capitan (10.11)** anymore. As this old version is not supported by Apple anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- Added: Official support for macOS Catalina (10.15)
- Removed: Support for Mac OS X El Capitan (10.11)
- Fixed: Reopening Word document fails if it has been externally modified in between
- Fixed: Excel cannot save files with square brackets in path
- Changed: Updated Chromium Embedded Framework to v75.1.14
- Changed: Updated BCFS to 3.10.3
- Minor bug fixes and improvements

Version 2.28.995 (2019-07-10)

- Added: French, Spanish and Italian localization
- Added: SharePoint Online & 2019 auto-detection
- Added: Apple Notarization Support
- Changed: Updated Chromium Embedded Framework to v73.1.12
- Changed: Updated BCFS to v3.10.1
- Fixed: Memory leak when running for a very long time
- Fixed: Very long encrypted filenames are not synced by Google Drive
- Fixed: Opening encrypted online-only files sometimes fails in Google Drive File Stream
- Fixed: Spotlight triggers on-demand file downloads
- Removed: Group Management (now available at boxcryptor.com)
- Removed: Edit Account (now available at boxcryptor.com)
- Removed: Master Key Generation (now available at boxcryptor.com)
- Removed: Cuda Drive (service does not exist anymore)
- Removed: Cubby support (service does not exist anymore)
- Minor bug fixes and improvements

Version 2.27.977 (2018-12-18)

- Added: Chromium Embedded Framework and replaced Safari WebView
- Added: Support for OneDrive On-Demand Files
- Improved: Faster sign-in and application start
- Fixed: Copying files with access control lists can fail
- Fixed: Copying application bundles to Google Drive File Stream can fail
- Fixed: Saving files with Excel to Google Drive File Stream can fail
- Minor bug fixes and improvements

Version 2.26.964 (2018-09-06)

This version has **official support for macOS Mojave (10.14)**.

This version **does not support Mac OS X Yosemite (10.10)** anymore. As this old version is not supported by Apple anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- Added: Official support for macOS Mojave (10.14)
- Removed: Support for Mac OS X Yosemite (10.10)
- Fixed: Boxcryptor crashes if Google Drive File Stream version 27.1.29.1732 is installed (can also result in "Mounting the Boxcryptor disk failed" errors)

Version 2.25.954 (2018-07-31)

- Added: Experimental support for macOS Mojave (10.14)
- Fixed: Cannot start on macOS 10.10
- Changed: Updated BCFS to v3.8.2

Version 2.24.941 (2018-06-14)

- Minor bug fixes and improvements

Version 2.23.939 (2018-05-24)

- Updated: Privacy Policy
- Fixed: Google Drive File Stream
- Minor bug fixes and improvements

Version 2.22.933 (2018-04-19)

- New: Multi-threaded filesystem
- Added: Russian localization
- Added: Dropbox Team Spaces support
- Added: Compatibility with VirusBarrier v10.9.16 or newer
- Fixed: Standalone OneDrive app is not auto-detected
- Minor bug fixes and improvements

Version 2.21.923 (2018-02-28)

- Fixed: Opening files can fail with Google Drive File Stream version 25.157.172.2329 and newer
- Minor bug fixes and improvements

Version 2.20.918 (2018-02-13)

- New: ownCloud and Nextcloud auto-detection
- Updated: Certificates used for certificate pinning
- Minor bug fixes and improvements

Version 2.19.907 (2017-12-13)

- Fixed: Too eagerly added some German texts which should be English.

Version 2.18.902 (2017-12-12)

- New: German localization
- Fixed: Wrong offline notification when adding a file to Google Drive File Stream in some cases
- Minor bug fixes and improvements

Version 2.17.892 (2017-11-23)

- New: Google Drive File Stream support
- New: Encryption Required policy
- Changed: Updated OpenSSL to v1.0.2m
- Minor bug fixes and improvements

Version 2.16.880 (880) (2017-10-09)

- Fixed: Volume could not be mounted on Mac OS X 10.10 Yosemite
- Fixed: "Finder integration missing" notification wrongly shown on macOS 10.13 High Sierra
- Fixed: Login failed under certain conditions on macOS 10.13 High Sierra
- Changed: Updated BCFS to v3.7.1
- Minor bug fixes and improvements

Version 2.15.875 (875) (2017-09-25)

> ℹ This version has official support for macOS High Sierra (10.13).

- New: Official support for macOS High Sierra (10.13)
- Added: "Apply to All" option when creating files or folders in unencrypted folders
- Improved: Compatibility with Arq backup software
- Changed: Updated BCFS to v3.7.0
- Minor bug fixes and improvements

Version 2.14.867 (867) (2017-08-28)

- New: Box Drive support
- New: Strato HiDrive auto-detection
- New: Nutstore auto-detection
- New: Disallow to manage permissions policy
- Improved: macOS 10.13 High Sierra support (experimental)
- Improved: Compatibility with Carbon Copy Cloner
- Improved: Automatic login to Whisply when using "Create Whisply Link" feature
- Changed: Boxcryptor drive is marked as case insensitive to properly reflect the already existing behavior
- Changed: Updated BCFS to v3.6.2
- Fixed: OneDrive and Google Drive Whisply link generation
- Minor bug fixes and improvements

Version 2.13.845 (845) (2017-06-20)

> ℹ This version has experimental support for macOS High Sierra (10.13).

- New: Support for custom certificate pinning allowing to use Boxcryptor in networks with SSL interception performed by e.g. anti-virus software or proxy servers
- New: Experimental support for macOS High Sierra (10.13)
- New: OneDrive for Business Germany support

Version 2.12.843 (843) (2017-01-06)

> This version does not support OS X 10.9 Mavericks anymore. As this old version is not supported by Apple anymore, we recommend affected users to update their operating system to a newer version as soon as possible in order to stay safe.

- Improved: Migrated to Dropbox API v2
- Fixed: Files or folders with names having certain asian characters at the beginning are not shown in the Boxcryptor drive
- Major redesign of the user interface for creating accounts and signing in
- Minor fixes and improvements

Version 2.11.828 (828) (2017-04-25)

- Fixed: Password protection has always been enabled after upgrading from a previous version (Tip: You can disable password protection in Preferences -> Security at any time.)
- Fixed: Internal RednifManager helper crashed when starting or quitting Boxcryptor
- Various other bug fixes and improvements

Version 2.10.820 (820) (2017-04-19)

- Added: Additional TouchID, PIN protection and reworked password protection
- Added: Support for Whisply with OneDrive for Business
- Fixed: Creating Whisply links for Google Drive sometimes failed
- Fixed: Trash does not work on non-default macOS user accounts
- Fixed: Mount could fail for macOS user accounts within Active Directory environments
- Fixed: Offline login did not work for users with many groups
- Fixed: Occasional "File not found" error when encrypting an existing folder
- Changed: Moved encryption preferences from "Advanced -> Encryption" to new "Security" tab
- Changed: Upgraded BCFS to v3.5.8
- Minor bug fixes and improvements

Version 2.8.800 (800) (2017-03-20)

- Added: Support for Dropbox Smart Sync
- Added: Plaintext overlay icon
- Fixed: Bulk operations (e.g. Manage Permissions) did not handle filename encrypted files or folders with "Umlaute" correctly
- Fixed: Sometimes temporary folders were not deleted when saving a file in MS Office 2016
- Fixed: Saving an encrypted MS Office 2016 file in an unencrypted folder could remove encryption (to avoid any such situation, it is always recommended to store encrypted files within an encrypted folder)
- Fixed: Boxcryptor drive did freeze under certain circumstances
- Changed: Upgraded BCFS to v3.5.6
- Changed: New provisioning profile valid until 2035

- Minor bug fixes and improvements

Version 2.7.778 (778) (2016-11-12)

- Updated: Certificates used for certificate pinning
- Fixed: File handle leak when managing permissions
- Minor bug fixes and improvements

Version 2.6.775 (775) (2016-11-07)

- Minor bug fixes and improvements

Version 2.5.774 (774) (2016-10-31)

- Added: Filename encryption can be enabled or disabled on existing folders. (Right-click -> Boxcryptor -> Enable/Disable filename encryption)
- Added: Check and fix Boxcryptor permissions directly via the Manage Permissions Window
- Added: Duplicate file hiding resolving to automatically rename files and folders hiding other items
- Added: Referral attribution when the referred user creates his account with Boxcryptor for macOS (by reading the default's browsers cookies for boxcryptor.com)
- Fixed: Preferences screen is not always correctly updated on remote changes
- Changed: The Patch number has been removed from the versioning scheme so that it has been changed from Major.Minor.Patch (Build) to Major.Minor.Build (Build). New releases will always increment the Minor number instead of the Patch number.
- Various other bug fixes and improvements

Version 2.4.403 (768) (2016-09-28)

- Fixed: Trash and Spotlight did sometimes not work in v2.4.401.758
- Fixed: Various app crashes on 10.12 Sierra
- Changed: Upgraded BCFS to v3.5.2
- Various other bug fixes and improvements

Version 2.4.401 (758) (2016-09-22)

> This version does not support OS X 10.7 Lion and 10.8 Mountain Lion anymore. As these old versions are not supported by Apple anymore, we recommend affected users to update their operating system to a newer version as soon as possible in order to stay safe.

- Added: macOS 10.12 Sierra support (official)
- Fixed: Automatic detection of OneDrive did not always work correctly
- Changed: Upgraded BCFS to v3.5.1
- Changed: Dropped support for OS X 10.7 Lion and 10.8 Mountain Lion
- Various other bug fixes and improvements

Version 2.3.405 (746) (2016-08-05)

- Fixed: Spotlight does not include results from Boxcryptor drive in v2.3 versions.
- Improved: Reliability of Finder extension

- Changed: Upgraded BCFS to v3.4.1
- Changed: Due to unexpected issues with Spotlight, the Boxcryptor drive is again mounted under /Volumes instead of the home directory. The new mountpoint is /Volumes/Secomba/{USERNAME}/Boxcryptor where {USERNAME} is the currently logged in macOS username. By default, a symlink is created from ~/Boxcryptor to the new mountpoint and it is recommended to only reference the ~/Boxcryptor symlink in custom scripts to be independent from future mountpoint changes.
- Various other bug fixes and improvements

Version 2.3.403 (737) (2016-07-21)

- Added: Granting and revoking group ownership by right-clicking on a group member
- Fixed: Missing "Do you want to encrypt" dialog on copying or moving files to an unencrypted folder
- Fixed: Cannot create a Whisply link in OneDrive
- Various other bug fixes and improvements

Version 2.3.401 (733) (2016-07-07)

- Added: Whisply integration
  Transfer files securely end-to-end encrypted in Dropbox, OneDrive and Google Drive with a simple link.
- Added: Icon overlays
  Encrypted files and folders are no longer marked with a green tag but instead have icon overlays.
- Added: Support for multiple operating system users
  Boxcryptor is now mounted in the user's home folder so that it can now be used by every user on a Mac and is not limited to a single user anymore.
- Added: macOS 10.12 Sierra support (experimental)
  Secure your data on Apple's latest operating system
- Improved: Faster sign in
- Improved: No internet connection required to work in folders shared permissions
- Improved: Updated to BCFS v3.4.0
- Changed: Boxcryptor now mounts at ~/Boxcryptor instead of /Volumes/Boxcryptor. If you want to keep old paths, you can manually create a symlink from /Volumes/Boxcryptor to ~/Boxcryptor. **(UPDATE 08/05/2016: This change had to be partially reverted in v2.3.405 due to unexpected issues with Spotlight. The new mountpoint is now /Volumes/Secomba/{USERNAME}/Boxcryptor)**

> The v2.3.x versions will be the last versions with Mac OS X 10.7 & 10.8 support. They are not actively supported by Apple anymore and we strongly encourage every user who is still using any of these old, unsecure operating systems to upgrade to a newer, secure version.

Version 2.1.467 (718) (2016-02-12)

- Added: Hidden preference "disableAccessControlLists" in order to disable the newly introduced support for Access Control Lists (ACLs) which could give a small performance boost if they are not required.
- Fixed: Sporadic deadlock when accessing ACLs on a symlink whose target is located on the Boxcryptor drive

- Fixed: Sporadic deadlock when setting attributes on a symlink whose target is located on the Boxcryptor drive
- Fixed: If a folder contains an item with a filename represented by more than 255 bytes, also other items are possibly not shown in the Boxcryptor drive. Now only the affected item is not shown but all other items are displayed correctly. In order to show the affected item, shorten its original filename.
- Minor bug fixes and improvements

Version 2.1.465 (708) (2016-01-25)

- Fixed: Cannot remove an ACL from a file or folder.
- Improved: Updated BCFS to v3.1.0
- Improved: Updated OpenSSL to v1.0.2e

Version 2.1.463 (707) (2016-01-18)

- Added: Auto-detection for the next generation OneDrive for Business sync client.
- Added: Support for Access Control Lists (ACLs).
- Minor bug fixes and improvements

Version 2.1.461 (704) (2015-12-16)

- Added: Auto-detection for LiveDrive.
- Added: Support for email addresses with gTLDs.
- Removed: Auto-detection for Wuala.
- Fixed: The file name of an encrypted Office document does not keep its encryption setting if the document is saved within a plain text folder.
- Fixed: Changing the case of a file or folder name deletes it under certain circumstances.
- Fixed: LiveDrive syncing causes Boxcryptor to create lots of files.
- Fixed: Cannot save a Office document when the path exceeds 255 characters.
- Minor bug fixes and improvements

Version 2.1.459 (701) (2015-11-16)

- Changed: When renaming a plaintext file/folder in an encrypted folder, it is not being encrypted anymore.
- Improved: Reduced memory usage when reading/writing whole files (e.g. using Encrypt/Decrypt with Boxcryptor in the context menu).
- Improved: Updated BCFS to v3.0.9
- Fixed: When getting the value of the extended attribute com.apple.ResourceFork the position parameter was not used correctly.
- Fixed: Reading the last file block did not always return the correct last 16 bytes when it was a full block.
- Fixed: Cannot checkout a repository via Git
- Minor bug fixes and improvements

Version 2.1.457 (697) (2015-10-28)

- Added: Hidden preference "autoDetectRemovableDrives" in order to disable the auto-detection of removable drives
- Fixed: Do not auto-detected mounted disk images as removable drives
- Improved: Updated BCFS to v3.0.8
- Minor bug fixes and improvements.

Version 2.1.455 (695) (2015-10-23)

- Fixed: Boxcryptor drive does not open if the system user account is connected to an Active Directory
- Minor bug fixes and improvements.

Version 2.1.453 (692) (2015-10-15)

- Changed: Trash is automatically emptied when the user disables the Trash.
- Fixed: Mounting timed out because the network destination of an alias on the Desktop is not available and cannot be resolved in the given time.
- Fixed: File descriptors leak when trying to access encrypted files without permissions.
- Fixed: Files with encrypted filenames which contain decomposed UTF-8 characters cannot be accessed.
- Minor bug fixes and improvements.

Version 2.1.451 (688) (2015-10-07)

- Fixed: High CPU load and unusable Boxcryptor drive on OS X 10.11 El Capitan when Path Finder is running
- Minor bug fixes and improvements.

Version 2.1.449 (685) (2015-09-24)

- Added: Support for OS X 10.11 El Capitan
- Added: Support for App Transport Security
- Improved: Better support for new gTLDs
- Improved: Updated BCFS to v3.0.6
- Fixed: Rsync failed if the source folder contained Apple double files
- Minor bug fixes and improvements.

Version 2.1.447 (677) (2015-08-18)

- Added: Auto-detection for Copy.com Sync and Copy.com CudaDRIVE.
- Improved: Boxcryptor drive aliases on the Desktop and Finder can now be removed without having to modify a hidden preference. When any of these aliases is deleted or removed, you will be asked if it should be recreated, or not.
- Minor bug fixes and improvements.

Version 2.1.445 (674) (2015-07-10)

- Minor bug fixes and improvements.

Version 2.1.443 (672) (2015-07-02)

- Added: Preliminary support for Mac OS X 10.11 El Capitan (beta)
- Added: Auto-detection for removable devices (e.g. usb flash drives)
- Fixed: Minimized impact of OS X XARA keychain vulnerability by always re-creating keychain items instead of updating existing items.
- Fixed: Finder can't open Excel documents on network locations in some cases.
- Fixed: Deadlock of the Boxcryptor disk when running an executable from the disk.

- Improved: Updated BCFS 3.0.4

Version 2.1.441 (667) (2015-05-07)

- Fixed: Word for Mac Preview (2015) fails to save documents in the Word 97-2004 format (.doc)
- Minor bug fixes and improvements.

Version 2.1.439 (664) (2015-04-30)

- Added: Auto-detection for Wuala.
- Fixed: Master key cannot be unlocked when the company administrator is excluded from the policy.
- Fixed: Crash when creating a group or editing permissions of a file or folder under certain circumstances.

Version 2.1.437 (663) (2015-04-28)

- Added: Auto-detection for OneDrive for Business.
- Improved: Extended attributes are now preserved when encrypting / decrypting a file or folder via right-click "Encrypt / Decrypt with Boxcryptor".
- Fixed: OneDrive auto-detection is broken after SkyDrive has been renamed to OneDrive.
- Fixed: A location cannot be added when another location's folder name contains parts of its name (e.g. /OneDrive and /OneDriveBusiness).
- Fixed: Various applications (e.g. Excel, Word, Filemaker) cannot save a file under certain circumstances (was introduced in version 2.1.435.654).
- Minor bug fixes and improvements (also from build 660).

Version 2.1.435 (654) (2015-04-07)

- Added: Auto-detection for iCloud when used in combination with the new Boxcryptor for iOS version 2.4. Files which should be available on mobile (iPhone/iPad) must be stored in the "iCloud" location. Files which are stored in the "iCloud Drive (Mac & PC only)" location are not accessible on mobile devices due to restrictions by Apple.
- Fixed: "Failed to load key holder" in the manage permission screen under certain circumstances.
- Fixed: Crash when modifying permissions if the user does not have direct access (e.g. only via a group).
- Improved: Write performance if an application expands the file before writing file contents.
- Minor bug fixes and improvements.

Version 2.1.433 (652) (2015-03-24)

- Fixed: Powerpoint cannot open files in the Boxcryptor drive.

Version 2.1.429 (648) (2015-03-16)

- Added: Filename encryption inheritance. New file or folders now inherit the filename encryption setting of their parent folder. If the name of the parent folder is encrypted (or not), the name of the new file or folder will also be encrypted (or not) - regardless of the filename encryption setting of the user.
- Improved: Updated to BCFS v3.0.2.

Version 2.1.427 (646) (2015-03-10)

- Added: Auto-detection for providers with multiple folders (e.g. Dropbox for Business).
- Added: Finder sidebar icon.
- Improved: Sign in speed.
- Improved: Excel save process.
- Improved: Updated to BCFS v3.0.1.
- Changed: Files or folders with encrypted filenames which cannot be decrypted are not hidden by default anymore. This behavior can now be controlled in the advanced settings.
- Fixed: Dropbox sync icons are sometimes not shown on Yosemite when Boxcryptor is running.
- Fixed: Zero size of Boxcryptor drive if only a WebDAV locations available.
- Minor bug fixes and improvements.

Version 2.1.425 (631) (2015-01-19)

- Fixed: Crash on OS X 10.7 Lion on startup.

Version 2.1.425 (630) (2015-01-14)

- Changed: Update check now submits a fake UDID instead of the real device UDID.

Version 2.1.423 (629) (2014-12-27)

- Added: "Show Boxcryptor Encrypted File/Folder" and "Show Boxcryptor Preferences" context menu entries for OS X Yosemite.
- Minor bug fixes and improvements.

Version 2.1.421 (628) (2014-12-24)

- Fixed: Files and folders cannot be moved between locations if they are on different devices.
- Minor bug fixes and improvements.

Version 2.1.419 (626) (2014-12-17)

- Fixed: Context menu is disabled in details view with expanded locations.
- Minor bug fixes and improvements.

Version 2.1.417 (625) (2014-12-12)

- Added: Prompt to disable VirusBarrier's Real-Time Scanning if required in order to avoid incompatibilities which can cause various problems (e.g. a "hanging" or forced unmounting of the Boxcryptor disk). It is **strongly** recommended to disable VirusBarrier's Real-Time Scanning and **not** to use Boxcryptor when it is enabled.

Version 2.1.415 (623) (2014-12-10)

- Improved: On Yosemite the Boxcryptor context menu is now located directly within the context menu and not in the "Services" menu anymore.
- Improved: On Yosemite the green tag of encrypted files is not copied anymore when copying or moving a file from the Boxcryptor disk to another location.
- Changed: Renamed auto-detected iCloud Drive location to "iCloud Drive (Mac & PC only)" to better guide users where they can access encrypted files in this location. Note: We are working on full iCloud support also on mobile devices which will be available in the next version of

Boxcryptor for iOS (ETA in January).
- Fixed: Problems when using Wuala
- Fixed: Boxcryptor disk can deadlock on accessing symlinks in the Boxcryptor disk which have a target in the Boxcryptor disk.
- Minor bug fixes and improvements

Version 2.1.413 (618) (2014-11-20)

- Fixed: Issue with desktop alias creation.

Version 2.1.413 (617) (2014-11-12)

- Fixed: The Boxcryptor disk is shown twice on the Desktop when mounted as local.

Version 2.1.413 (613) (2014-11-12)

- Improved: Better encryption / decryption performance by improved utilization of multi-core systems.
- Improved: The Boxcryptor disk is now always shown in the Finder favorites and on the Desktop.
- Improved: Modifying permission does now retain the original modification date (instead of setting it to the current date and time).
- Fixed: Enabling Spotlight fails under certain circumstances.
- Fixed: Sign out does not unlink the device
- Minor bug fixes and improvements

Version 2.1.411 (610) (2014-10-27)

- Added: "Temporary file preservation" for encrypted files is now also applied to plaintext filenames - not only encrypted filenames. This improves temporary file detection by other applications, e.g. to exclude them from sync.
- Improved: Updated icons for OS X 10.10 Yosemite.
- Improved: Increased mount / unmount timeout from 30 to 60 seconds.
- Minor bug fixes and improvements

Version 2.1.409 (603) (2014-10-22)

- Fixed: Offline login does not work on OS X 10.10 Yosemite.
- Fixed: Spotlight and Trash cannot be enabled under certain circumstances.
- Minor bug fixes and improvements

Version 2.1.407 (601) (2014-10-13)

- Fixed: Wrong key expired error message.
- Fixed: Freezing in certain circumstances.
- Fixed: Open file handle leak which can cause a too many open files error.
- Improved: Manage permission windows are now always kept in foreground.
- Various crashes fixed and overall stability improvements.

Version 2.1.405 (595) (2014-09-24)

- Fixed: "Unknown key server error" when upgrading from v2.0.xxx.
- Fixed: Occasional crash when enabling Spotlight on (Mountain) Lion.

Version 2.1.403 (592) (2014-09-23)

- Added: "Temporary file preservation" for encrypted filenames so that temporary files can be detected by other applications even with filename encryption.
- Improved: Reduced idle CPU load on OS X Yosemite.
- Improved: Performance of filename encryption through caching.

Version 2.1.401 (588) (2014-09-18)

- Added: OS X Yosemite support
- Added: iCloud Drive
- Added: Spotlight and Trash support
- Improved: Saving and loading of preferences
- Improved: Offline support and better stability in case of weak internet connection
- Improved: Replaced OSXFUSE with out own implementation BCFS. OSXFUSE is not required to run Boxcryptor anymore. BCFS will automatically be installed on the first start of Boxcryptor.
- Improved: Better handling for sync conflicts / conflicted copies. Encrypted filenames which have been modified (e.g. by appending a " (conflicted copy)") are now auto-fixed by including the suffix automatically into the encrypted filename. The conflicted copy then also appears in the Boxcryptor Disk.
- Overall stability improvements

Version 2.0.411 (566) (2014-02-20)

- Improved Permissions Management
- Detect Box Sync 4.0
- Encryption/Decryption of bundles/packages (when using the Finder Context Menu)
- Boxcryptor not showing Locations on WebDAV/SMB shares
- Minor UI fixes and improvements.

Version 2.0.409 (511) (2014-01-30)

- Added: Performance improvements on filesystem operation
- Fixed: Some file attributes not copied on Encrypt/Decrypt operations
- Fixed: Permission denied on some file operations
- Fixed: Duplicate names on folder decrypt operations
- Fixed: Various bug & crash fixes. • General performance and stability improvements

Version 2.0.403 (360) (2013-12-19)

- Added: Encrypt/Decrypt individual files (via Finder’s context menu).
- Added: Master Key (for Company Package users).
- Added: Help Menu.
- Fixed: “Remember password” not always working.
- Fixed: Allow user to choose if the crash logs are sent automatically
- Fixed: Various UI improvements, including Preferences & Manage Permissions
- Fixed: Other fixes and performance improvements, including lower memory usag

Version 2.0.401 (260) (2013-12-06)

- Minor bug fixes and improvements

Version 2.0.400 (250) (2013-12-05)

- Initial Release

Network Access

Boxcryptor requires that certain servers can be accessed via the internet. If you have network restrictions in place, please make sure to allow connections from Boxcryptor to the following domains, ip addresses, ports and protocols:

```
Domain: www.boxcryptor.com
Port: 443
Protocol: HTTPS
IP Adresses: 136.243.125.201, 148.251.224.98, 188.40.161.200
```

```
Domain: api.boxcryptor.com
Port: 443
Protocol: HTTPS
IP Addresses: 136.243.125.202, 148.251.224.99, 188.40.161.201
```

```
Domain: whisp.ly
Port: 443
Protocol: HTTPS
IP Address: 188.40.161.203
```

If you are using our LDAP / Active Directory synchronization feature, please make sure that your directory server can be reached from the following subnets: `136.243.125.192/28`, `148.251.224.96/28`, `188.40.161.192/28`.

Please note that these domains and also ip addresses might be subject to change in the future.

Open Source Licenses

We use open source software in many situations: across platforms in the Boxcryptor apps, in the Boxcryptor Crypto Server, and for boxcryptor.com. Follow the links below to view the list of open source projects and their licenses used in the corresponding applications:

- Boxcryptor for Windows
- Boxcryptor for macOS
- Boxcryptor for Android
- Boxcryptor for iOS
- Boxcryptor for Microsoft Teams
- Boxcryptor Crypto Server
- Boxcryptor Portable
- boxcryptor.com
- boxcryptor.com/app

- whisp.ly