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. Additionally, typical cloud storage features, such as file history or selective sync, are supported.

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.
- Boxcryptor is **not a sync client**, which means that Boxcryptor on Windows or macOS 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

System Requirements: Requires macOS 10.15 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.

To install Boxcryptor on your Mac, follow these steps:

1. Install the desktop application of your cloud provider.
2. Download Boxcryptor for macOS.
3. Open the downloaded installer file.
4. Drag and Drop the Boxcryptor icon to the Application folder.

ℹ **System Extension Required** Boxcryptor contains a system extension which is required to provide the Boxcryptor drive. As system extensions are blocked in macOS 10.13 and newer by default, you must **allow loading system software from developer "Benjamin Fleischer"** on first start. Benjamin is the maintainer of the open source system extension used by Boxcryptor.

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.

Create a Boxcryptor Account

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.

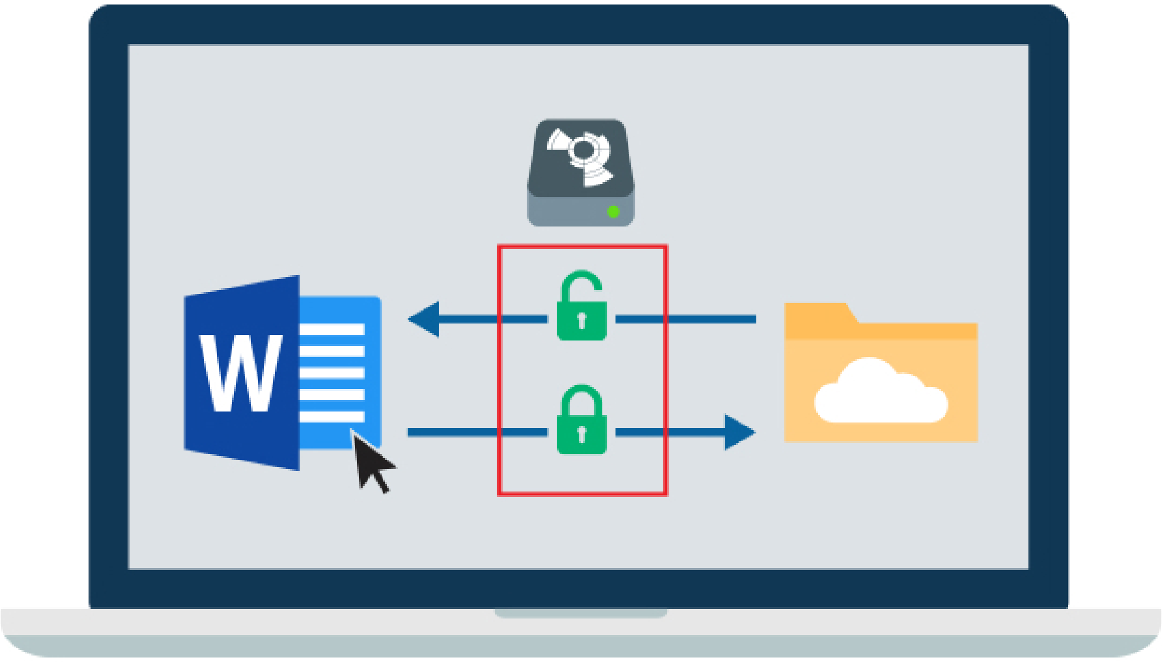
Create a password that you can remember, or store the password in a secure place, for example a password manager. Boxcryptor is a zero knowledge encryption software, therefore we **cannot** restore your password.

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

Discover Boxcryptor

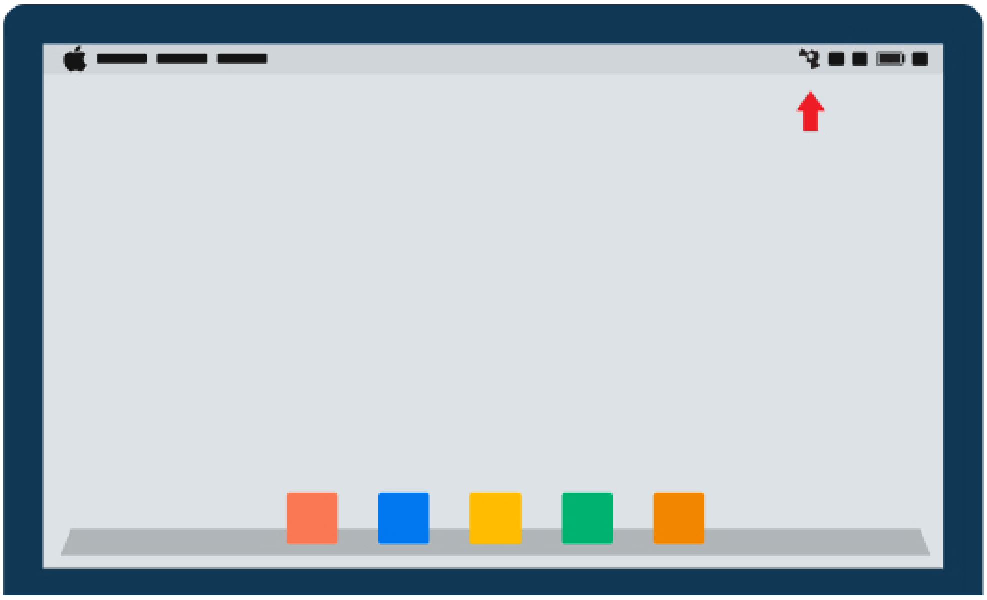
Once you have installed Boxcryptor and signed in to your account, you can access the **Boxcryptor drive**.

Boxcryptor will automatically add all installed cloud providers to the drive. From now on you can find all your clouds here. The drive acts like a layer on top of your existing files. It enables you to view, edit, and save your encrypted files on-the-fly.



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

Note: You can open your Boxcryptor Drive by clicking on the Boxcryptor logo in your menu bar, in the Finder sidebar or on your Desktop.



Your First Encrypted Folder

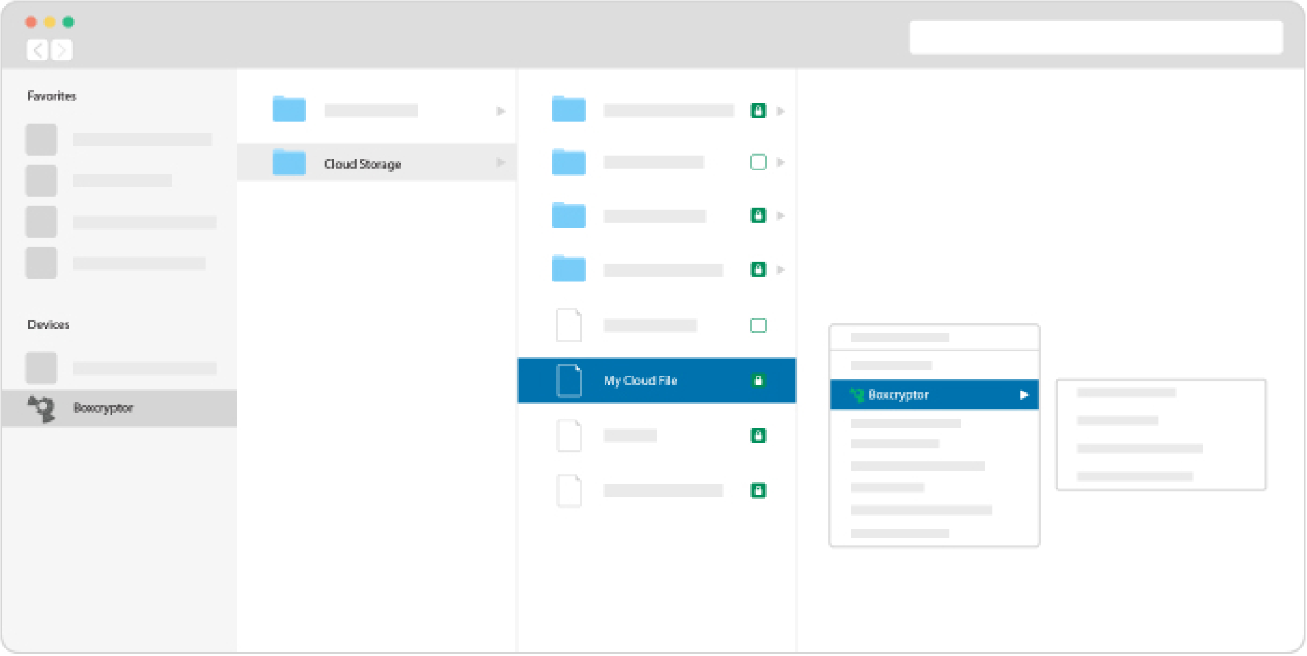
All files and folders that you add to an **encrypted folder** in Boxcryptor will be **encrypted automatically**. If you are new to Boxcryptor and do not have any files in your cloud yet, this is how you get started.

1. Open the **Boxcryptor Drive**.
2. Open the cloud provider's folder in the Boxcryptor drive.
3. **Right-click** into the folder → **New Folder**.
4. Click **yes** to confirm that you want to create an encrypted folder.
5. Add files to the folder and all files will be encrypted automatically.

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 drive**.
2. **Right-click** on a file or folder → **Boxcryptor** → **Encrypt**.
3. Wait for your cloud provider's sync client **to sync everything**.



ⓘ To prevent sync conflicts when encrypting existing folders, Boxcryptor will create a new folder with the suffix *_encrypted* and move your existing files into this new folder. The suffix can be safely removed after the folder has been synced by your cloud storage provider.

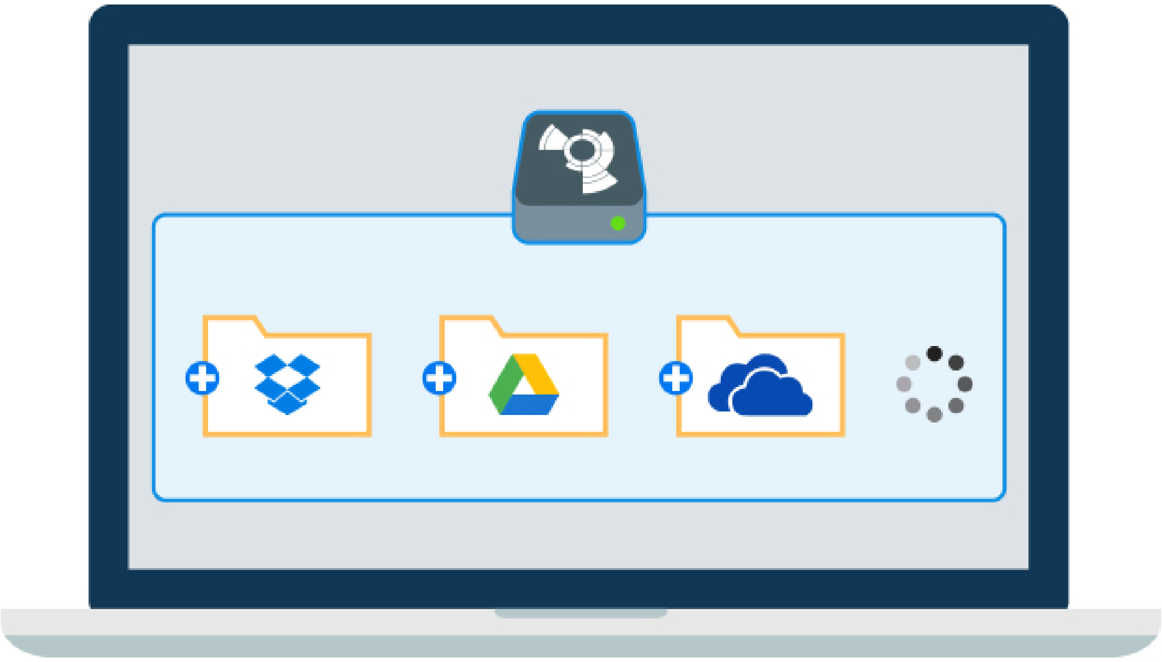
Manage Clouds and Locations

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.

Cloud Storages

Boxcryptor works as an **additional security layer** for your cloud storage. We handle the encryption, while the cloud storage's software syncs your files to the cloud. Therefore, **Boxcryptor requires the sync client of your cloud provider to be installed** on your system.

Most clouds are detected automatically by Boxcryptor, and added as a location to the Boxcryptor drive. If your cloud is not detected automatically, you can add it manually as a custom location.



Individual locations can be enabled or disabled via the Location settings. Right-click the **Boxcryptor menu bar icon** → **Preferences** → **Locations** and alter the checkboxes next to the cloud provider names as you need it.

Note: Free accounts can only activate one location. If you need more, please upgrade here.

Dropbox

Dropbox is not compatible with macOS 12.3 because the Dropbox client is not fully supporting Apple's latest operating system yet. If you choose to update to macOS 12.3, **you will experience issues opening online-only files** in Dropbox with some third-party apps. Dropbox will not automatically download them anymore.

The latest version of Boxcryptor contains a mitigation for this incompatibility so that opening encrypted online-only files works in Boxcryptor as expected. **We strongly recommend to use Boxcryptor version 2.46.1668 or newer on macOS 12.3.** The latest version of Boxcryptor can be downloaded here.

> Did you know about the next generation of Boxcryptor for macOS? It does not require a Dropbox client and fully supports macOS 12.3. Learn more about it in our blog.

OneDrive

Due to technical restrictions of the new OneDrive client with updated Files On-Demand experience, Boxcryptor cannot open encrypted online-only files on the first attempt. Online-only files are only available online and not locally on your Mac.

Thus, the first attempt to open an such an encrypted file in Boxcryptor always fails. At at the same time, Boxcryptor displays a corresponding notification and automatically triggers the download of the file. **After the file has been downloaded by OneDrive, it can be opened as usual in second and subsequent attempts as long as it is locally available on your Mac.**

Despite receiving an error message when you try to open an encrypted online-only file for the first time, **your encrypted data is never at risk.** OneDrive's updated Files On-Demand experience does not support downloading and opening encrypted files at the same time, so Boxcryptor must perform these actions separately. For locally available files, Boxcryptor works with OneDrive without any restrictions.

> We are working on a completely reworked Boxcryptor for macOS version which will not depend on the OneDrive sync client anymore. You can learn more about it here.

Google Drive

Boxcryptor automatically detects both your Google Drive **mirrored** and **streamed** locations. **Any additional backed up folder is not added automatically.**

> Only content synced using the **Google Drive** tab is available on other devices. Folders from **My Computer** are not accessible on other computers or in the mobile Boxcryptor apps. If you want to encrypt files in any backed up folder, you can manually add it as a custom location.

> **Shared Drives** are currently only supported in **streamed** locations.

Maximum file name length

While Google Drive itself does not have a maximum file name length limit and synchronizes any file name length **from a Mac to Google Drive**, it restricts the maximum file name length when synchronizing a file or folder **from Google Drive to a Mac**.

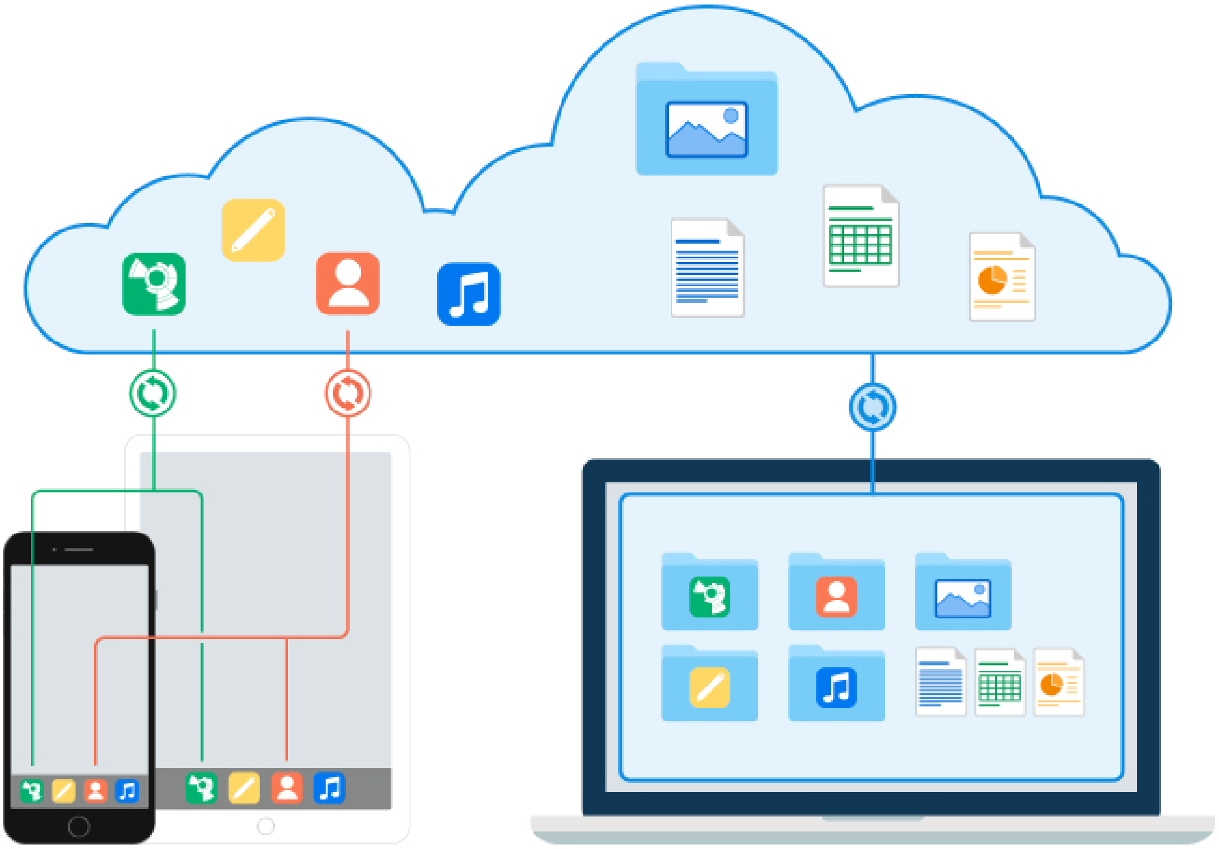
While **mirrored** locations have a maximum file name length of **255 bytes**, **streamed** locations allows only up to **250 bytes** for a file name. If a file name exceeds these limits, Google Drive synchronizes the file but truncates the name so that it meets the limit. Please note that the length is not limited in the number of characters, but the number of bytes required by the name. One character used by Boxcryptor's file name encryption can occupy up to 4 bytes.

If an encrypted file name is truncated, Boxcryptor cannot decrypt the file name anymore because the whole encrypted file name is required for successful decryption. In this case, **you must shorten the file name** so that it does not exceed Google Drive's limits and is not being modified by Google Drive.

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.

The fact that there is an iCloud Drive (a typical cloud provider) and an iCloud (where all your apps and their cloud space are managed by Apple) makes setting up encryption across platforms a little more complicated, compared to other clouds. Some additional steps are necessary in the beginning. But once your iCloud in combination with Boxcryptor is set up, working with the data is as simple as on other platforms.



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

How to encrypt iCloud Drive and make all your data available on mobile and desktop devices

If you want to have your encrypted data available on all your devices you have to take the following steps:

1. Install Boxcryptor on your iPhone or iPad and also on your desktop devices.
2. Make sure that you are signed in to iCloud on all devices.
3. Add the **iCloud** provider in Boxcryptor for iOS.
4. Upload an encrypted file to **iCloud** via Boxcryptor for iOS.
5. Apple will then create a Boxcryptor folder in their cloud.
6. Open Boxcryptor on your desktop and access the **iCloud** location on macOS or **iCloud Drive** → **Boxcryptor** on Windows. You will find the encrypted file from your iPhone or iPad there.
7. To make files from your Mac or PC available on your iPhone or iPad, move or copy the files to the folders mentioned above. You will then have them available on your mobile and desktop devices.

Files stored only in iCloud

Due to technical restrictions, Boxcryptor requires files to be downloaded and available on the Mac. Files available only in iCloud and not stored on the Mac are not available in the Boxcryptor drive. Those files must first be downloaded in iCloud Drive before they appear in the Boxcryptor drive.

I Cannot Activate the iCloud Location

Before you can activate iCloud as a location, please **add iCloud in your Boxcryptor for iOS app**. Upload a small dummy file so that the Apple System creates a Boxcryptor folder.

Network Drives and USB Devices

Removable USB drives are detected automatically by Boxcryptor, too.

Network drives are not yet automatically detected Boxcryptor. You can add network drives as a custom location as described below.

How to disable removable drive auto-detection

You can disable this feature by modifying the **autoDetectRemovableDrives** hidden preference.

Custom Locations

If your favorite cloud is not listed as a supported provider or if you want to encrypt a specific folder on your machine, you can add those as well:

Click the **Boxcryptor menu bar icon** → **Preferences** → **Locations** → + and then choose your very own location.

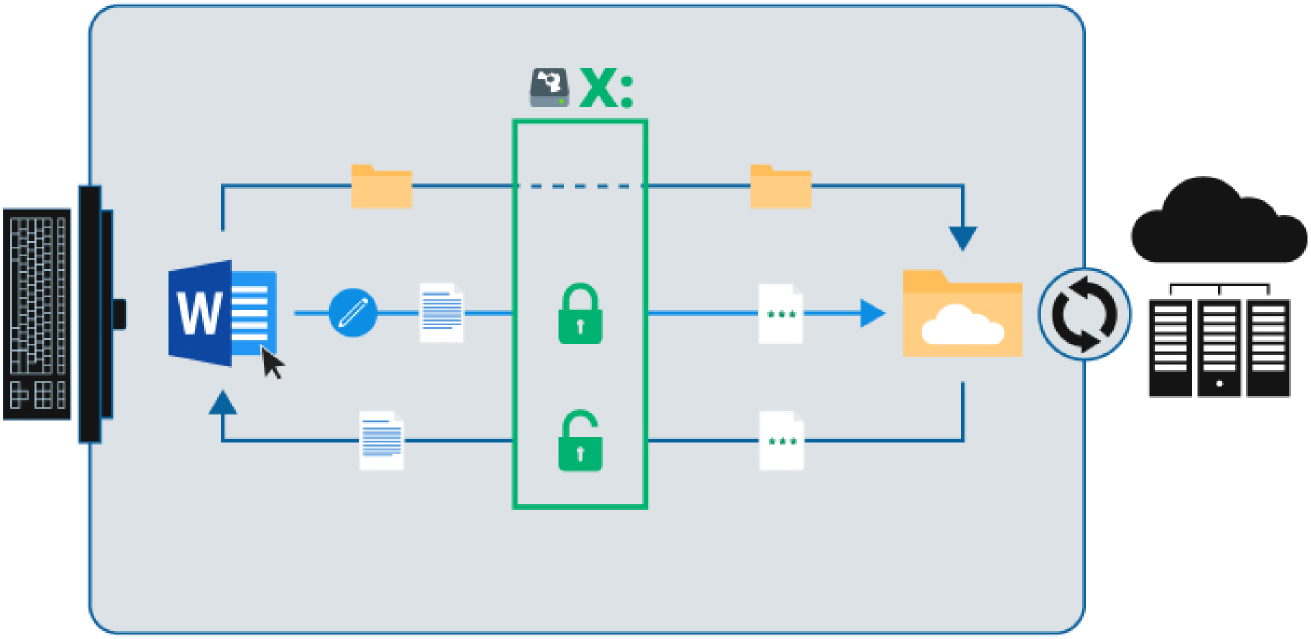
> If your chosen location is not a sync folder of a cloud provider, nothing will be uploaded to the cloud. The data stays on your PC locally, just like any other folder, but encrypted.

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.

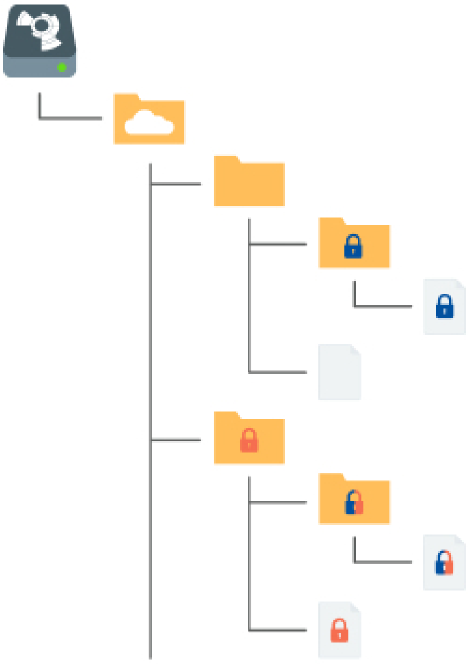


We accomplish this simplicity by creating a virtual drive on your machine. It acts like an **encryption-empowered window to your data**. All your files – whether they are encrypted or not – can be **accessed via this virtual Boxcryptor drive**.

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 ask you if you want to encrypt it or not.

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 by creating a virtual drive. 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 Drive 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 right-clicking the **file or folder → Boxcryptor → 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. All files and folders in the Boxcryptor drive are **marked with small icons** that indicate their current state.

🔒 **encrypted**

□ **not encrypted**

If you are using Dropbox Smart Sync (or another cloud which supports the on-demand feature) there are additional states and icons:

🔒 **encrypted** and **online only**

🔒 **encrypted** and the folder contains **both** encrypted and not encrypted files

☁ **not encrypted** and **online only**

☁ **not encrypted** and the folder contains **both** encrypted and not encrypted files

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.
- Right-click the selection and chose **Boxcryptor** → **Encrypt** in the context menu.
- Wait for your cloud provider's sync client to sync everything.

> Please **wait until your cloud provider's client synchronized your files to the cloud**, before you start working with them. This helps to prevent sync conflicts.

Note: To improve synchronization results, Boxcryptor adds an **_encrypted** suffix to the names of the files and folders you encrypt. After synchronization is completed, you can rename them.

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: 恂悰挦抱砻掺殯栯瞻擟豉漢快搬濂檬浉楻掭抧柜榉眇.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 **Boxcryptor Preferences → Security → Encryption** and check **Enable filename encryption**.

To change the filename encryption settings of already encrypted items, right-click them and select **Boxcryptor → Enable / Disable filename encryption** in the context menu. Follow the instructions and make sure to let the files sync completely before you continue to work with them.

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 right-click on the file or folder you want to decrypt and select **Boxcryptor → Decrypt**.
- If you want to copy or move your files to another location in decrypted mode, just select the files in the Boxcryptor drive with the Finder and copy or move them to the new location. The data will be decrypted automatically.

On-Demand Files

Some cloud providers offer that not all files are automatically synced to your device. Instead, only the directory structure is replicated on your device and files are download on demand when you open them. This saves valuable disk space and bandwidth while still being able to access every file from your computer.

Dropbox Smart Sync

Dropbox Smart Sync defines three states for files and folders:

- **Online-only content** shows in your local Dropbox folder, but doesn't use the full amount of space that the file would. In your file explorer, you can see the file, but the content isn't fully downloaded until you need it. Only information about the file, such as the file name, location, and date the file was updated, is downloaded.
- **Mixed state folders** contain both local and online-only content.
- **Local content** is downloaded and saved on the hard drive of your computer. You can directly edit these files from applications on your computer.

Boxcryptor preserves the Smart Sync state of files in Dropbox, downloads files via Dropbox on-demand when another application opens an online-only file and displays the Smart Sync state in the Boxcryptor drive.

Files and folders are **marked with small icons** that indicate their current state.

Note: The Dropbox Smart Sync state of folders is determined only by taking into account the files at the first level. Files in subfolders are omitted for performance reasons.

Opening online-only files

You can browse to an online-only file in the Boxcryptor drive and directly open it. Boxcryptor will immediately trigger a download via Dropbox Smart Sync and waits until it finished. After the download finished, the file open process will continue. If the download takes more than 3 seconds, Boxcryptor will abort the file open operation in order to preserve the responsibility of the Boxcryptor drive. The download progress will be shown directly in Finder and once the download has finished, you can re-try to open the file.

Downloading online-only files

If you want to make an online-only file locally available without having to open it, you can right-click any online-only file and choose **Boxcryptor → Download.** Please note, that it is currently not possible to revert this operation, i.e. make a locally available file online-only, or to download a complete folder (only single files) due to restrictions from Dropbox. If you'd like to perform this action, please perform it using the Dropbox application. You can select the original item directly in the Dropbox folder by right-clicking it and choosing **Boxcryptor → Show Original in Dropbox**.

Can I manage permissions of online-only folders?

Permissions are persisted in a file named FolderKey.bch within a folder. When this file is online-only, it will be automatically downloaded by Dropbox when opening the Manage Permission dialog in Boxcryptor. If the file cannot be downloaded because there is no internet connection, permissions cannot be changed at that time. In this case, go online and try it again.

Why can opening an Office application (Word, Excel, Powerpoint) be very slow?

When you open an Office application, it tries to read all recently opened files. If these files are online-only, Dropbox downloads them and blocks the opening application until the download has finished. Clearing your recently opened files list in the Office application resolves this issue.

Why are certain files always local even after I made them online-only?

Please see the the question above. When a file is included in the recently opened file list of an Office application, opening the application will always cause Dropbox to download them. Clearing your recently opened files list in the Office application resolves this issue.

When do I need an internet connection while working with Smart Sync enabled?

You need an internet connection when trying to open an online-only file or working in an encrypted folder whose folder key file (FolderKey.bch) is online-only. We recommend to always make an encrypted folder completely locally or online-only available and avoid having mixed state folders when you anticipate a bad internet connection.

Can I make a file or folder online-only in the Boxcryptor drive?

No, it is currently not possible to make a file or folder online-only when you are in the Boxcryptor drive. If you want to make a file or folder online-only, you must go directly to the Dropbox folder and choose **Smart Sync** → **Online Only** in the Dropbox context menu. To identify a file or folder in the Dropbox folder, you can right-click the item in the Boxcryptor drive and choose **Boxcryptor** → **Show Original** in Dropbox.

Can I download a folder in the Boxcryptor drive?

No, it is currently not possible to download a folder in order to make it locally available when you are in the Boxcryptor drive. If you want to make a folder locally available, you must go directly to the Dropbox folder and choose **Smart Sync** → **Local** in the Dropbox context menu. To identify a file or folder in the Dropbox folder, you can right-click the item in the Boxcryptor drive and choose **Boxcryptor** → **Show Original** in Dropbox.

Can I use Spotlight to find online-only files?

You can find online-only files by name, but it is not possible to find them by their content because online-only files do not contain any content.

Google Drive File Stream

Google Drive File Stream is officially supported by Boxcryptor on all platforms. Find more information on our blog.

Box Drive

Box Drive is also officially supported by Boxcryptor.

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

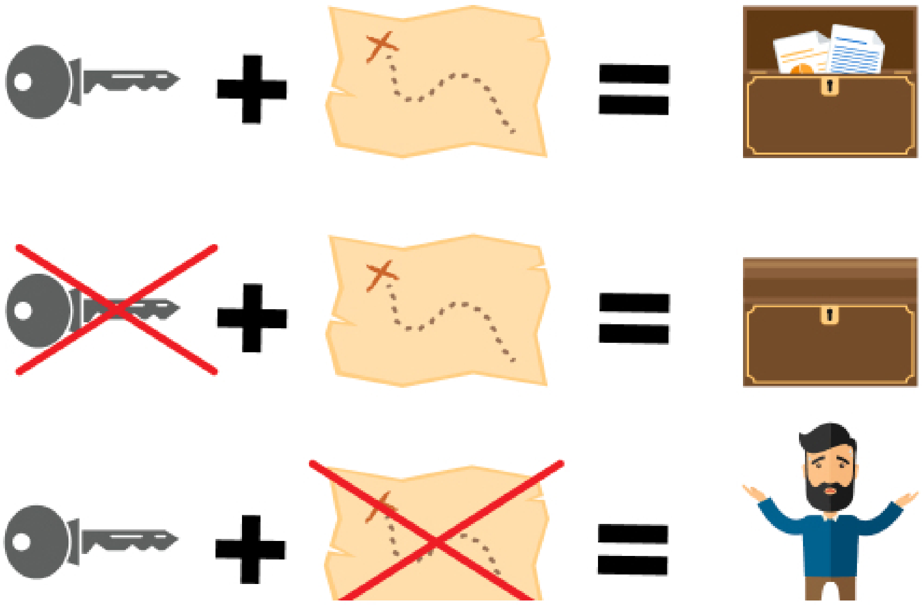
For understanding how the sharing of encrypted files works, it is helpful to understand how programs handle unencrypted and encrypted files.

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**.

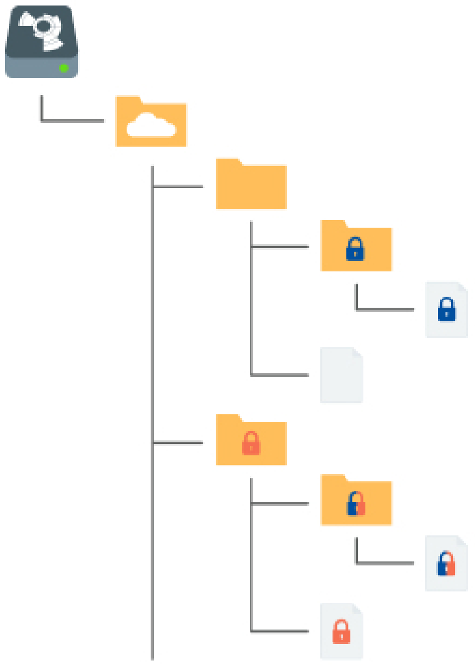
As a consequence, there are two steps necessary to share an encrypted file:

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:

- Right-click the **file or folder** → **Boxcryptor** → **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.
- Right-click the file or folder again → **go to Boxcryptor** → **Show Original at Provider**.
- Right-click the original folder → **Share**.

> 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 managing your users and their access rights. The group management is availaible within the account by signing in on our website.

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 permissions in the files do not change, synchronization is not necessary.

Settings

App Protection

App protection prevents **unauthorized access** to Boxcryptor.

If this feature is activated, you can set **several authentication methods**. You have to authenticate yourself with a set method to use Boxcryptor.

You can enter an invalid authentication up to five times. If you fail to authenticate yourself, you have to enter your Boxcryptor password or reset Boxcryptor to factory settings.

These are the authentication methods you can choose from:

- **4-digit PIN code**: When set, you have to enter a 4-digit PIN code.
- **Password**: When set, you have to enter your Boxcryptor password.
- **Touch ID and device password**: When set, the user must enter his or her fingerprint by using the device's fingerprint sensor. This feature is only available on devices that support Touch ID. Apple provides a fallback to Touch ID, that allows you to use the device's password instead of Touch ID if you prefer.

Boxcryptor requires you to enter the authentication at start. Afterwards, Boxcryptor will run until you specifically quit the software. If you want to protect Boxcryptor when you are away from your device, please use your operating system's features to lock your device manually or automatically after certain amount of time.

You can activate and set up the protection feature in the settings: **Boxcryptor menu bar icon → Preferences → Security**.

Note: If an attacker gains access to your operating system, it is theoretically possible for him to modify the locally stored Boxcryptor settings in such a way that the protection feature can be circumvented. 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

To access the Boxcryptor settings, click the Boxcryptor icon located in the menu bar and select Preferences. Navigate to the **Advanced** or the **Updates** tab to change autostart- and update settings.

The default settings are:

- Automatically check for updates

- Automatically send Diagnostic and Usage Data

Additionally, you can make the following changes to the Boxcryptor settings:

> ⚠ Changing these settings may cause unwanted behavior of Boxcryptor. Please do **not** change these unless you are an **experienced user**.

- **Mount for all users**: System accounts will be able to access Boxcryptor.
- **Mount as fixed disk**: Even though the Boxcryptor drive is a virtual drive, this option will make it look and treated as a real drive.
- **Enable trash**: Deleting files will move them to trash, so that they can be restored if necessary.
- **Enable Spotlight**: Enables spotlight to index and find files in Boxcryptor.

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 Switch Back to an Online Boxcryptor Account

If you initially started with a local account but want to profit from all the benefits a full Boxcryptor account offers, you can convert your local account to a regular Boxcryptor account here.

This only works if you don't have an online Boxcryptor account already.

If you temporarily use a local account with your exported keys and want to switch back, you can simply **sign out** of Boxcryptor and sign back in with your online account. Assuming **you did not perform an Account Reset**, your files will still be accessible.

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

1. Click ••• on the sign in screen.
2. Choose **local account**.
3. Click on **I want to use a local account**.
4. Drop your key file into the gray area.
5. Enter your password to sign into Boxcryptor.

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**.

> ℹ 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

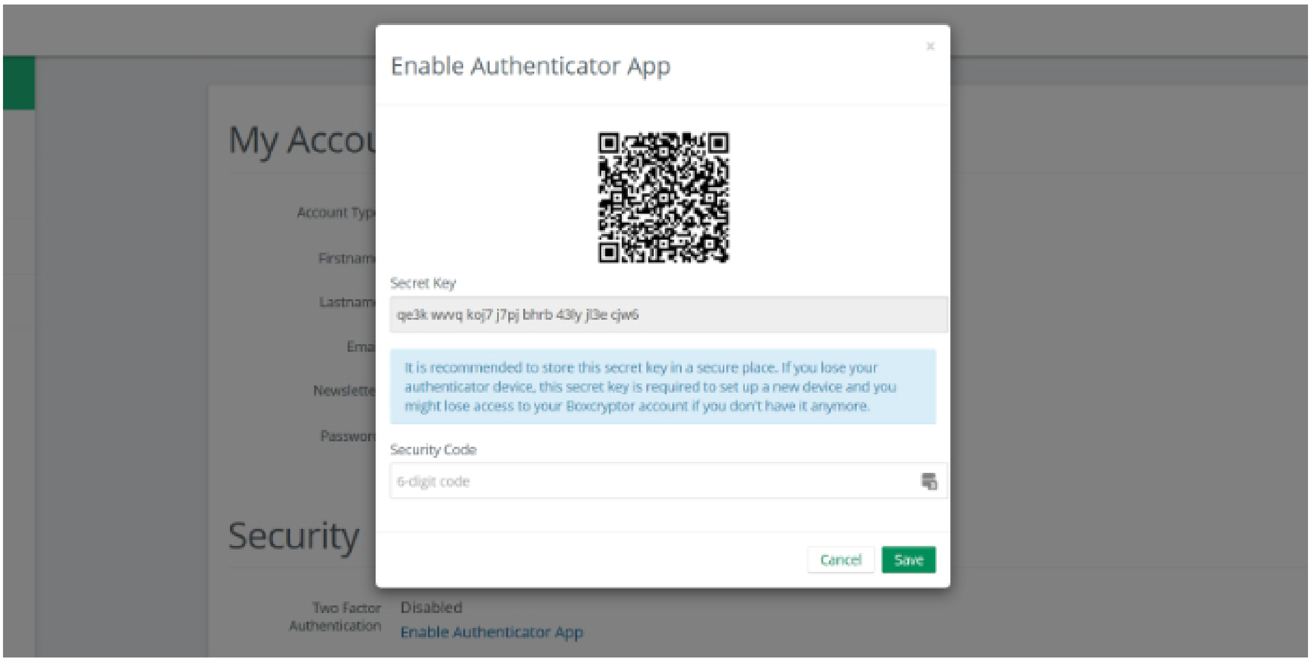
Authenticator apps use the Time-based One-Time Password algorithm (TOTP) to generate secure 6-digit code on your mobile device which have to be entered during authentication. To use it, **you need to install an Authenticator App** of your choice on your mobile device. Next, you need to configure both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

Two Factor Authentication: Disabled

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

> 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.

> 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

New Boxcryptor for macOS Beta

Which macOS versions are supported?

The new Boxcryptor for macOS Beta only **supports the latest macOS 12 Monterey**. Versions prior macOS 12 Monterey (e.g. Catalina or Big Sur) are not supported.

Which Macs are supported?

All current Macs, e.g. MacBook Air & Pro, Mac mini & Pro or iMac, with **Intel and Apple Silicon (M1) processors are supported**.

Where can I get the Beta?

The Beta is available via Testflight. Follow these steps to install the new Boxcryptor for macOS Beta:

1. Install Testflight from the Mac App Store: https://apps.apple.com/us/app/testflight/id899247664
2. Install Boxcryptor via Testflight (Link only works in Safari): https://testflight.apple.com/join/DA2T1TyF

Are special instructions required for the installation?

No, the new Boxcryptor for macOS Beta is a native “File Provider” app which works “out-of-the-box" on modern macOS operating systems. Because it does not use a kernel extension anymore, it is not required to modify the Mac's Security Policy and the installation does not require rebooting the device. Additionally, the app is now fully utilizing the macOS sandboxing security mechanism.

If you changed your Mac’s Security Policy to Reduced Security due to a previous Boxcryptor for macOS version, you can revert this policy back to Full Security when you exclusively use the new Boxcryptor for macOS Beta 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

Can I use the Beta for production data?

No, we recommend not to use the Beta on production systems or with production data. The Beta is a pre-release software which may contain errors or inaccuracies and may not function as well as a final version. Be sure to have backups of the data you're using with the new Boxcryptor for macOS Beta.

With the Beta, we want to give interested users and customers early access to the future of Boxcryptor and users can give us early feedback and an opportunity to shape of Boxcryptor for macOS.

Where are files encrypted?

As you expect from 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 in the past, **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

Where can I find Boxcryptor on my Mac?

In previous versions of Boxcryptor for macOS, the Boxcryptor drive was mounted on the path `/Volumes/Secomba/[USERNAME]/Boxcryptor` and accessible via shortcuts in Finder's Favorite section, in the user's home folder and on the Desktop.

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.**

Do I still need my cloud provider's client on my Mac?

No, the new Boxcryptor for macOS version **now includes the full functionality for fast, smooth and secure synchronization of your files and folders.** The new Boxcryptor for macOS version is all you need installed on your Mac to work with encrypted files in Dropbox, OneDrive, Google Drive or any other supported cloud provider. When using the new Boxcryptor for macOS Beta, you can remove your cloud provider's client from your Mac.

Why is everything new?

A main driver for the new Boxcryptor for macOS version is Apple's strategy to disallow third party kernel extensions in macOS in order 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 possibilites and experiences this new integration into macOS opens up for Boxcryptor in the future.

Can I use Spotlight again?

Yes, finally! 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 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.

> ℹ In the first version of the new Boxcryptor for macOS Beta, Spotlight can only index contents of folders that you have previously navigated to. In the stable version, all folder contents will be indexed by Spotlight even if they have never been accessed in Finder.

Which limitations are known?

The following limitations are currently known and will be resolved until the final version of the new Boxcryptor for macOS app:

Context menu is not yet supported, including the following features:

- Managing permissions is not yet supported

- Creating Whisply-Link is not yet supported
- Encrypting/Decrypting of existing items is not yet supported

Can the new Beta and a previous version of Boxcryptor for macOS be used at the same time?

Yes and no. You can rename a previous version of Boxcryptor for macOS (e.g. from "Boxcryptor.app" to "Boxcryptor Legacy.app") and then install the new Beta to have both versions installed on your Mac at the same time. However, it is not possible to start and use both versions at the same time without interferences. Switching between them one at a time might also lead to unexpected problems, e.g. being signed out on the next start.

We recommend to stick to one version for most of the time and only switch if explicitly required, e.g. in order to modify permissions of an encrypted folder using a previous version of Boxcryptor for macOS.

When will the new Boxcryptor for macOS version officially be available?

The Beta will be continuously improved in the coming weeks and is scheduled to be replaced by a stable version in the first half of 2022.

How to 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** and send it to us via support@boxcryptor.com

Please be aware that the logs contain meta-information about your file and folder structure, including tags, file names, file sizes, etc. However, they do not contain file contents.

Boxcryptor is Using a Lot of CPU

CPU usage is completely dependent on the activity within the Boxcryptor drive. When many operations are executed within the Boxcryptor drive – such as reading and writing files – CPU usage will rise. When there is no activity in the Boxcryptor drive, there should not be any CPU usage.

However, it is **possible that those activities are kind of invisible**, for example when apps are running operations in the background, without the user's interaction. A classic example for that is the indexing service of Spotlight.

Boxcryptor is Slow

An App is Slower Than Usual When Used With Boxcryptor

When an app is slower than usual when used in combination with Boxcryptor, the app might have a problem with handling Boxcryptor's encryption. Boxcryptor simply acts as a filter, taking read and write requests from the operating system, and encrypting them on the way.

Well written apps write their files in blocks. In this case, Boxcryptor only needs to be active a few times during encryption and performance is not affected. Some apps, however, write each byte one by one. This results in many calls to Boxcryptor and leads to slower performance.

If you have trouble with one of your regular apps and performance is your priority, you could try out an alternative, to check if it can deal with Boxcryptor's encryption better.

A Background Process is Causing High Load

Slow performance of the Boxcryptor drive might be caused by a background process performing a huge amount of file operations on the Boxcryptor drive without the user noticing. As Boxcryptor is then busy handling all the file operations of the background process, Boxcryptor has less time to handle file operations of other application and thus might feel slow. A classic example for a background service causing high load on the Boxcryptor drive is a search indexing service, e.g. Spotlight.

Anti-virus software real-time scanning incompatibilities

The real-time scanning feature of anti-virus software intercepts file operations and scans them for malware behavior. This can lead to incompatibility problems with the virtual Boxcryptor drive when the anti-virus software intercepts file operations on the virtual Boxcryptor drive as well as all file operations performed by Boxcryptor itself. This can lead to serious performance problems or even freeze the whole Boxcryptor drive.

If you encounter any problems with the Boxcryptor drive or its performance and are using an anti-virus software on your Mac, disable the real-time scanning feature or exclude the Boxcryptor drive if possible. You may also contact the support for your anti-virus software vendor and report this incompatibility so that they can fix it.

Icons or the Context Menu are Not Shown

With macOS 10.10 Yosemite Apple introduced new App Extensions to add custom functionality for example to Finder. Since version 2.3.401 (733) Boxcryptor for macOS, the integration of Boxcryptor into Finder is implemented as a Finder Sync extension as recommended by Apple. The Finder integration includes the Boxcryptor context-menu available when right-clicking a file or folder within Boxcryptor in Finder and overlay icons which reflect the encryption status of files and folders in Boxcryptor. Unfortunately, the reliability of Finder extensions in general does not always meet the expected level and it can happen that the Finder integration is missing for obscure reasons which we cannot influence and can only be fixed by Apple. In this article, we will outline some actions you can take if you should be affected by this problem.

Before digging deeper into the problem, we'd recommend to perform the following actions which might already resolve your problem:

- **Relaunch Finder**: Hold down the option key and right-click the Finder icon the Dock to click Relaunch
- **Restart your Mac**: Click the Apple icon in the menu bar and choose Restart.
- **Reinstall Boxcryptor**: Stop Boxcryptor if it is running, download the latest version of Boxcryptor for macOS, open the Boxcryptor Installer image and copy the Boxcryptor app to your Applications folder.

If the Boxcryptor Finder integration is still missing, go to **System Preferences → Extensions** and verify that Boxcryptor is listed in your Finder extensions. If the Boxcryptor Finder extension is not listed at all, a general problem with Finder extensions on your Mac could be the reason. A strong indicator for this reason is also when there isn't any (Finder) extension listed at all and also Dropbox and other extensions are missing. The best advice in this case is to contact Apple support for help - but if you'd like to troubleshoot the problem yourself, here are a few things you could try:

Manually add the Boxcryptor Finder extension

Normally, macOS should automatically discover and install the Boxcryptor Finder extension when Boxcryptor is being started for the first time. In some rare cases, this is not the case and the extension is not automatically loaded. To fix this, you can try to manually add the extension by following these steps:

1. Open the **Terminal** application.
2. Execute the following command:
   ```
   pluginkit -a /Applications/Boxcryptor.app/Contents/PlugIns/Rednif.appex
   ```

Temporary disabling System Integrity Protection

System Integrity Protection (SIP) is an essential and important new protection mechanism introduced with macOS 10.11 El Capitan to prevent malware from tinkering with your operating system. Unfortunately, SIP also seems to sometimes break the extension system of macOS and we have seen reports where temporary disabling SIP, extensions could be loaded again and continue to load after SIP has been re-enabled. You should be really careful when modifying SIP and know the implications of your actions - information about SIP can be found here and here.

How to disable System Integrity Protection

CAUTION: We do generally not recommend to disable any system protection mechanism. Only perform these steps if you know what you do and on your own risk.

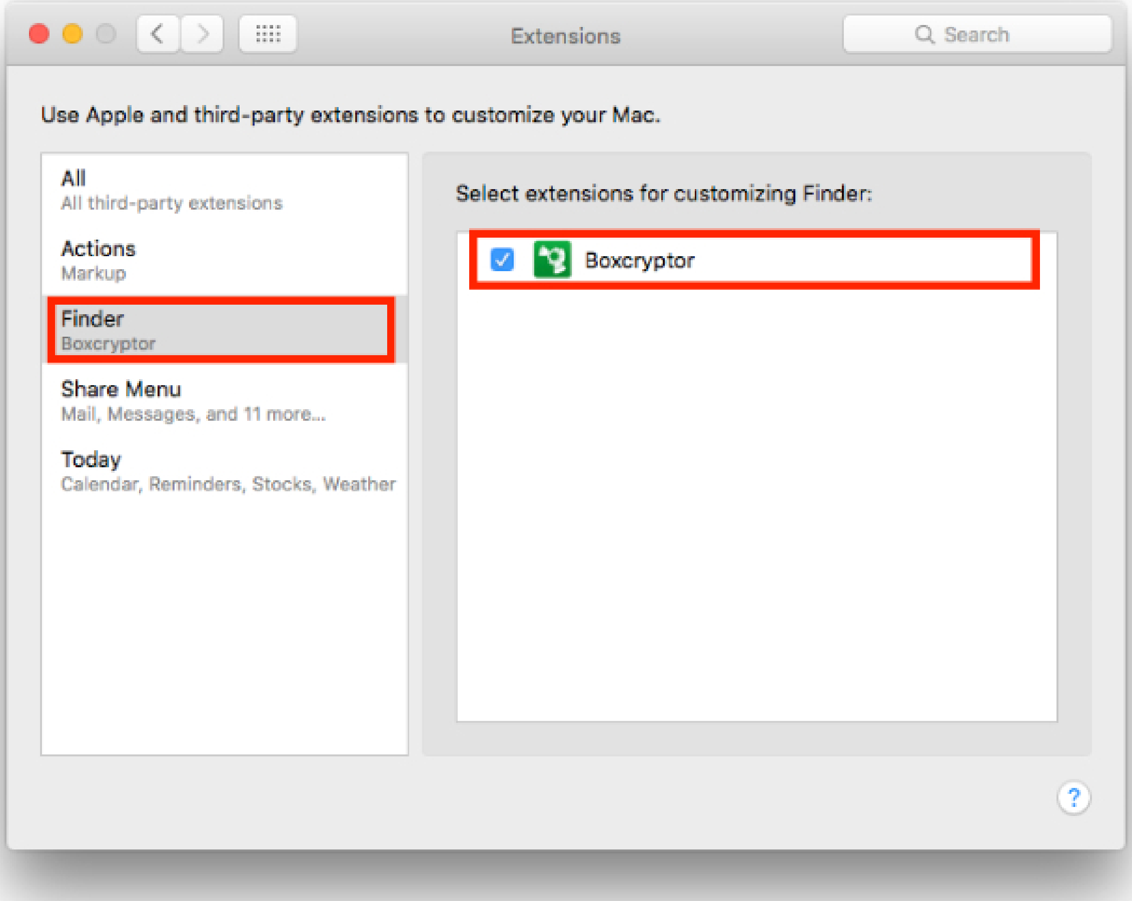
1. Reboot your Mac and hold down **Cmd+R** simultaneously in order to boot into **Recovery Mode**.
2. In the macOS Utilities screen, open **Utilities** and click **Terminal**.

3. Determine the current state of SIP by entering the following command: `csrutil status`.
4. Disable SIP by entering the following command: `csrutil disable`.
5. Reboot your Mac and verify that extensions have been loaded
6. Reboot your Mac into Recovery Mode again, open the Terminal and re-enable SIP by entering the following command: `csrutil enable`.

Reinstall macOS

We have seen reports where reinstalling macOS fixes the problem and extensions are loaded successfully again after the operating system has been set up freshly. Especially if extensions are missing in general (e.g. also the Dropbox extension is missing although it is installed), a reinstallation of macOS might be the only solution to get the extension subsystem working correctly again.

Ensure that the Boxcryptor Finder extension is enabled


Extensions
Search
All
All third-party extensions
Actions
Markup
Finder
Boxcryptor
Share Menu
Mail, Messages, and 11 more...
Today
Calendar, Reminders, Stocks, Weather
?

Use Apple and third-party extensions to customize your Mac.

Select extensions for customizing Finder:

☑ Boxcryptor

If the Boxcryptor Finder extension has been loaded and is listed in **System Preferences → Extensions**, verify that it is enabled and that the checkbox is checked.

Avoid extension conflicts

At any given time, only a **single** extension can be active for a specific folder regardless how many extensions are enabled. If two extensions register for the same folder, only one of them will be available in Finder and other will be ignored depending which extension was loaded first by macOS.

Try to disable other extensions in order to find possible conflicts. We have seen reports where especially the Google Drive and Synology Cloud Station Finder extensions caused problems with other extensions.

> ⓘ If none of these tips help and the Boxcryptor Finder integration still does not work on your Mac, we might be able to help you if you contact us directly. But you can be sure that you are not alone and we hope that Apple will fix extensions in the future.

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?

> ⓘ Having trouble with the latest **Boxcryptor for macOS Beta**? You can find instructions to create a log here (under section **How to create a debug log?**)

- Quit Boxcryptor.
- Open the **Terminal** app and execute the following command:
  `/Applications/Boxcryptor.app/Contents/MacOS/Boxcryptor --debug`

- Reproduce all steps that lead to the unexpected behavior.
- Quit Boxcryptor by clicking on the menu bar icon → **Quit Boxcryptor**.

A debug log (`Boxcryptor-<Timestamp>.rawnsloggerdata`) is generated and saved to **~/Library/Logs/Boxcryptor**.

How Do I Access the log folder?

- Open **Finder** and choose **Go** → **Go to Folder... (Cmd+Shift+G)**.
- Enter `~/Library/Logs/Boxcryptor` and click on go.

What Should I Do With my Debug Log?

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

ⓘ As debug logs can grow pretty big pretty fast, we recommend to compress the debug log file in order to reduce its size before sending.

Additional System Information

If your system configuration matters, you can export information about it as follows:

1. Open **Spotlight** → write `System Information` → press **Enter**. The system information overview opens.
2. In the menu bar go to `File` → `Save` to export the information and send it to us additionally.

Log filesystem accesses before execution

In rare cases it can be of interest to log accesses to the Boxcryptor drive before the file operation is carried out. To do so, check eager logging on how to enable it.

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: The Internet connection appears to be offline

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 offline. All files will be available. However, you will not be able to alter Boxcryptor permissions or use other online features of Boxcryptor.

How Do I Uninstall Boxcryptor?

Since Boxcryptor is deeply integrated into macOS and the system does not provide any uninstall mechanism by default, follow this guide to remove Boxcryptor completly from your system.

1. Quit Boxcryptor.
2. Open the **System Preferences** → **Extensions** → **Finder** 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.

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

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.

Advanced Client Configuration

Some preferences of Boxcryptor are not exposed in the user interface. While it is generally not recommended to modify these preferences, experienced users or administrators might want to do it to better tailor Boxcryptor to their needs.

⚠ The hidden preferences are loaded when Boxcryptor is starting. If Boxcryptor is running when you modify a hidden preference, you have to restart Boxcryptor in order for the change to be applied. Also be aware that the key is case-sensitive.

How to Manage Hidden Preferences

Hidden preferences are stored in the standard macOS user defaults system and can be managed using the **defaults** command in the Terminal application. The user defaults of Boxcryptor for macOS are stored in the domain "com.boxcryptor.osx". To manage the hidden preferences, you can execute the following commands in Terminal. Please read the man pages for the **defaults** command to learn more about using it.

- **defaults read com.boxcryptor.osx KEY** Reads the current value of KEY
- **defaults write com.boxcryptor.osx KEY VALUE** Stores VALUE for KEY
- **defaults remove com.boxcryptor.osx KEY** Deletes the KEY

List of hidden preferences

- **autoDetectRemovableDrives** By default, Boxcryptor auto-detects removable drives and automatically adds them as locations. Set this value to "NO" in order to disable the auto-detection of removable drives. Default: YES
- **disableAccessControlLists** By default, Boxcryptor supports access control lists (ACLs). Set this value to "YES" in order to disable this support if you don't need it. As getting ACLs requires additional file operations, disabling support for ACLs could slightly improve the performance of Boxcryptor. Default: NO
- **disableAliases** By default, Boxcryptor creates aliases for the Boxcryptor disk in the Finder sidebar and on the Desktop if Finder would not show it otherwise. Set this value to "YES" in order to disable the creation of aliases by Boxcryptor. Default: NO
- **disableDesktopAlias** By default, Boxcryptor creates an alias for the Boxcryptor disk on the Desktop if Finder would not show it otherwise. Set this value to "YES" in order to disable the creation of the Desktop alias by Boxcryptor. Note: Boxcryptor only creates the alias if Finder does not show connected servers (the Boxcryptor disk is mounted as remote disk). Please disable Finder -> Preferences -> General -> Connected servers in this case. Default: NO
- **disableSidebarAlias** By default, Boxcryptor creates an alias for the Boxcryptor disk in the Finder sidebar if Finder would not show it otherwise. Set this value to "YES" in order to disable the creation of the Finder sidebar alias by Boxcryptor. Default: NO
- **disablePlainTextWarning** By default, Boxcryptor will ask if you want to encrypt a file or folder if you create/copy/move it in a plaintext folder. You can disable this behaviour by setting this value to "YES". Boxcryptor will then always create plaintext files/folders in plaintext folders and not ask for encryption. Important: In this case, only files or folders created/copied/moved to already encrypted folders will be encrypted. Default: NO
- **hidePlaintextFilesFromSpotlight** By default, all files and folders within the Boxcryptor disk will be indexed by Spotlight if it is enabled. By setting this value to "YES", Spotlight will see and index only encrypted files and ignore any plaintext files in the Boxcryptor disk. Default: NO
- **revertFileModificationDateOnPermissionChange** When modifying permissions of encrypted files or folders, Boxcryptor will add a few seconds to the modification date so that synchronization apps can better detect and sync this change. If you do not want the modification date to change when modifying permissions in Boxcryptor, you can set this value to "YES". Boxcryptor will then revert the modification date to its original value after applying the new permissions. Default: NO
- **eagerLogging** By default, when logging is enabled, Boxcryptor logs filesystem events *after* being executed on the virtual Boxcryptor drive. By setting this value to "YES", Boxcryptor will also log the filesystem event *prior* to execution.

Examples

- **defaults write com.boxcryptor.osx disableAliases -bool YES** Disables the automatic creation

of Finder sidebar and Desktop aliases for the Boxcryptor disk.
- **defaults remove com.boxcryptor.osx disableAliases** Restore the default behaviour of Boxcryptor regarding alias creation.

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.

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.

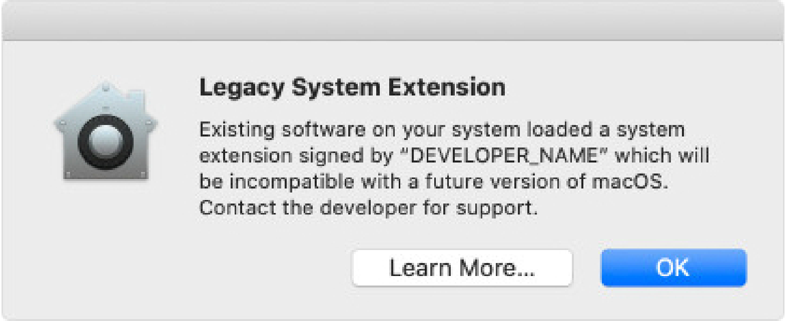
There has been an incompatibility with Dropbox in the past that could create "broken" content for smaller files because Dropbox did not sync the last file change.

- 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.

Legacy System Extension

System extensions have been used for many years to extend the functionality of macOS. In order to improve security, stability and reliability of macOS, Apple is currently working on modern alternatives to system extensions in future versions of macOS.

Boxcryptor uses a system extension to provide the virtual Boxcryptor drive. Therefore, you may receive a "Legacy System Extension" message when Boxcryptor starts for the first time and periodically when it is running beginning with macOS 10.15.4 (Catalina).



Legacy System Extension

Existing software on your system loaded a system extension signed by "DEVELOPER_NAME" which will be incompatible with a future version of macOS. Contact the developer for support.

We are aware of this message and Apple's transition away from system extensions in macOS. We will be ready to comply with Apple's future requirements in time.

Until then, you can ignore this message and safely close the window. Boxcryptor will continue working in macOS without any issues. More information can be found here.

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.

Enable System Extensions

> Enabling system extensions is a hard requirement to use Boxcryptor on Apple Silicon Macs and Boxcryptor will not work otherwise.

Apple is further locking down macOS in Apple Silicon Macs where 3rd party kernel extensions are disabled by default. Boxcryptor uses a kernel extension to provide the virtual Boxcryptor disk and integrate in macOS' file system for the best user experience. Only a kernel extension can offer this tight integration into macOS at the moment.

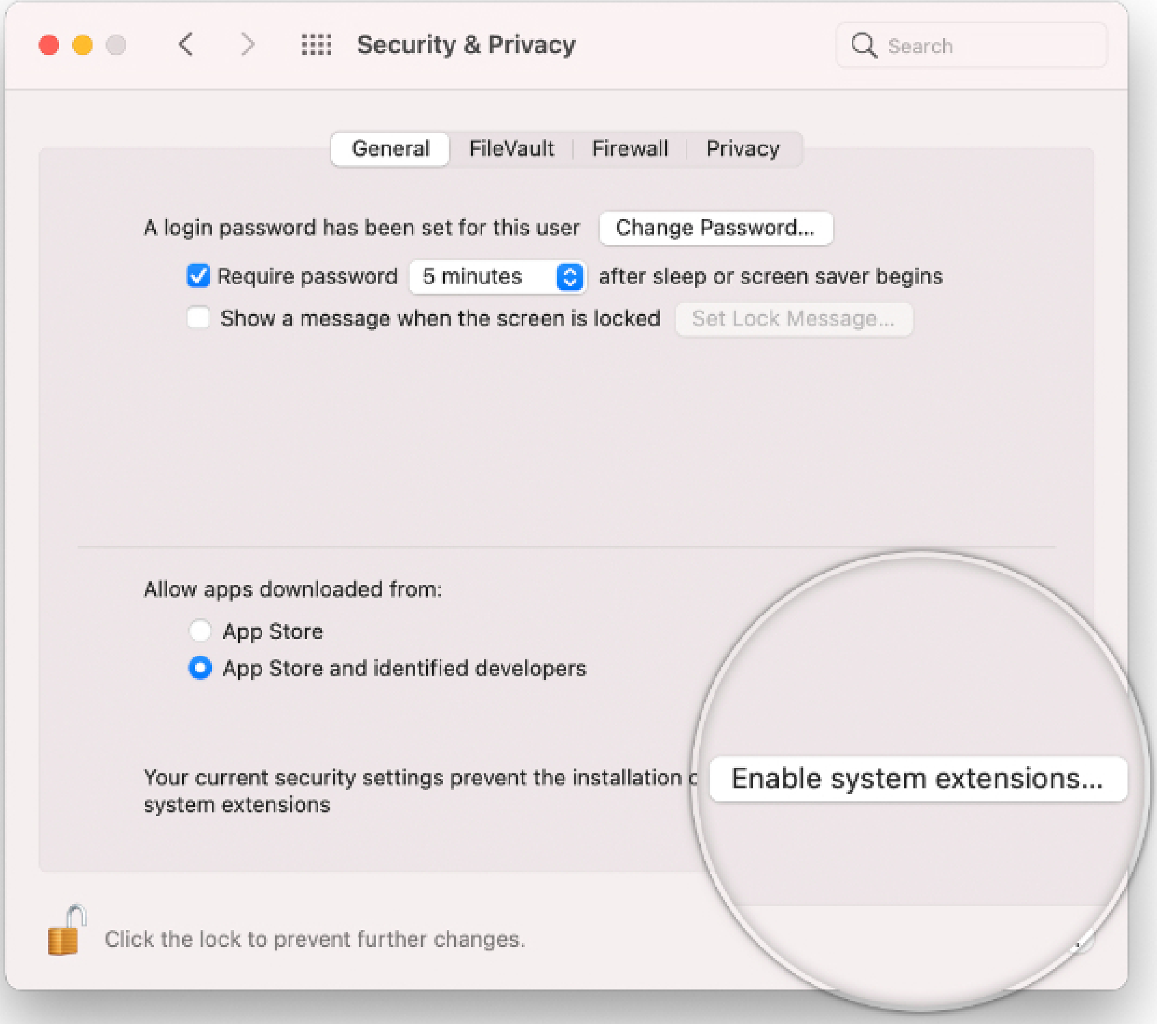
In order to use 3rd party kernel extensions on Apple Silicon Macs, users must enable system extensions by changing their Mac's **Security Policy** to **Reduced Security** and **allow user management of kernel extensions from identified developers**. Despite the dramatic name, **Reduced Security** still offers best-in-class security for every Mac:

In **Full Security**, only the latest Apple approved and signed version of macOS can be installed. When (re-)installing macOS, your Mac connects to Apple's servers and checks if the macOS version is allowed to be installed. Apple can remotely prevent the installation of a macOS version.

In **Reduced Security**, only Apple approved and signed versions of macOS can be installed. In contrast to **Full Security** this includes not only the latest, but also previous versions of macOS. No connection to Apple's servers is required and Apple cannot remotely prevent the installation of a macOS version.

Similar, allowing user management of kernel extensions from identified developers does not inheritly weaken the security of your Mac. **Kernel extensions are still blocked by default and every kernel extension must explicitly be approved by a user with administrator rights before it can be loaded.** Additionally, kernel extensions must be signed and notarized by Apple approved and accredited developers.

You will automatically be prompted to enable system extension when running Boxcryptor for the first time on an Apple Silicon Mac if required. In this case open **System Preferences -> Security & Privacy** and follow the provided instructions.



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

Allow apps downloaded from:

○ App Store

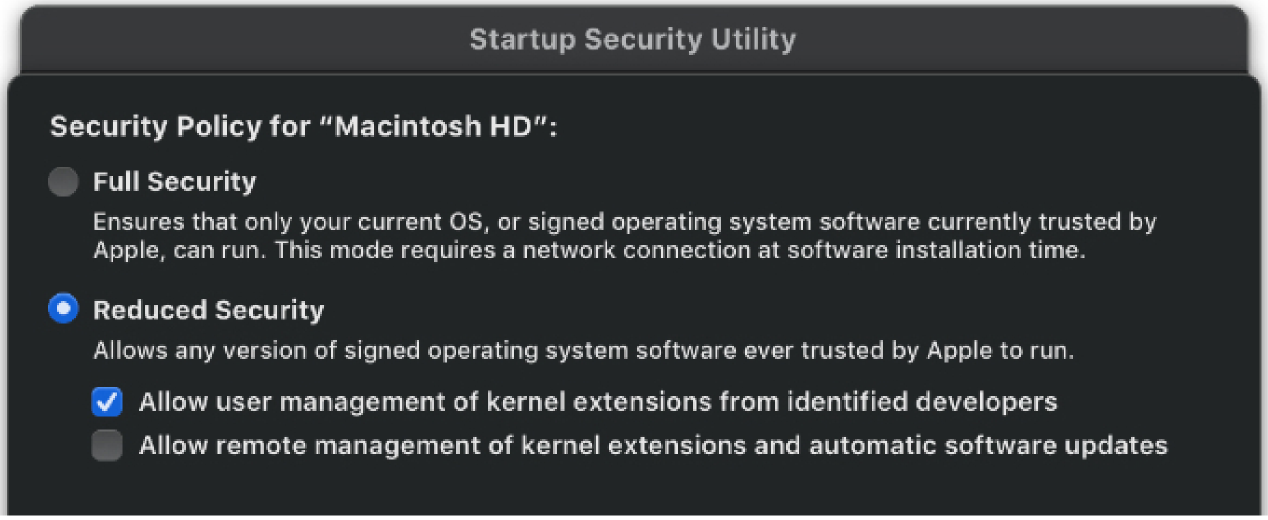
● App Store and identified developers

Your current security settings prevent the installation c system extensions

Click the lock to prevent further changes.

Alternatively, you can enable system extensions by following these steps as documented by Apple:

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 **Reduced Security**
5. Enable **Allow user management of kernel extensions from identified developers**
6. Click **OK** and confirm the action by entering your administrator credentials
7. Restart your Mac



Security Policy for "Macintosh HD":

○ Full Security

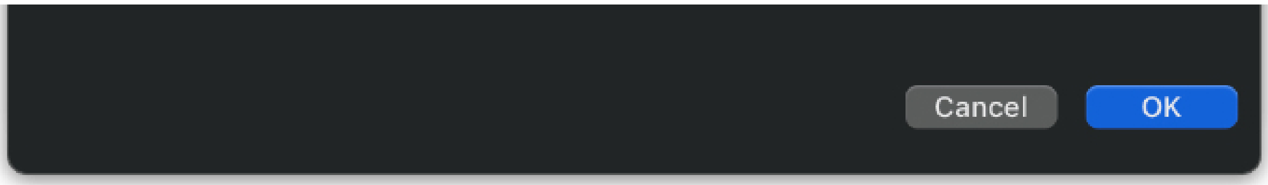
Ensures that only your current OS, or signed operating system software currently trusted by Apple, can run. This mode requires a network connection at software installation time.

● Reduced Security

Allows any version of signed operating system software ever trusted by Apple to run.

☑ Allow user management of kernel extensions from identified developers

□ Allow remote management of kernel extensions and automatic software updates

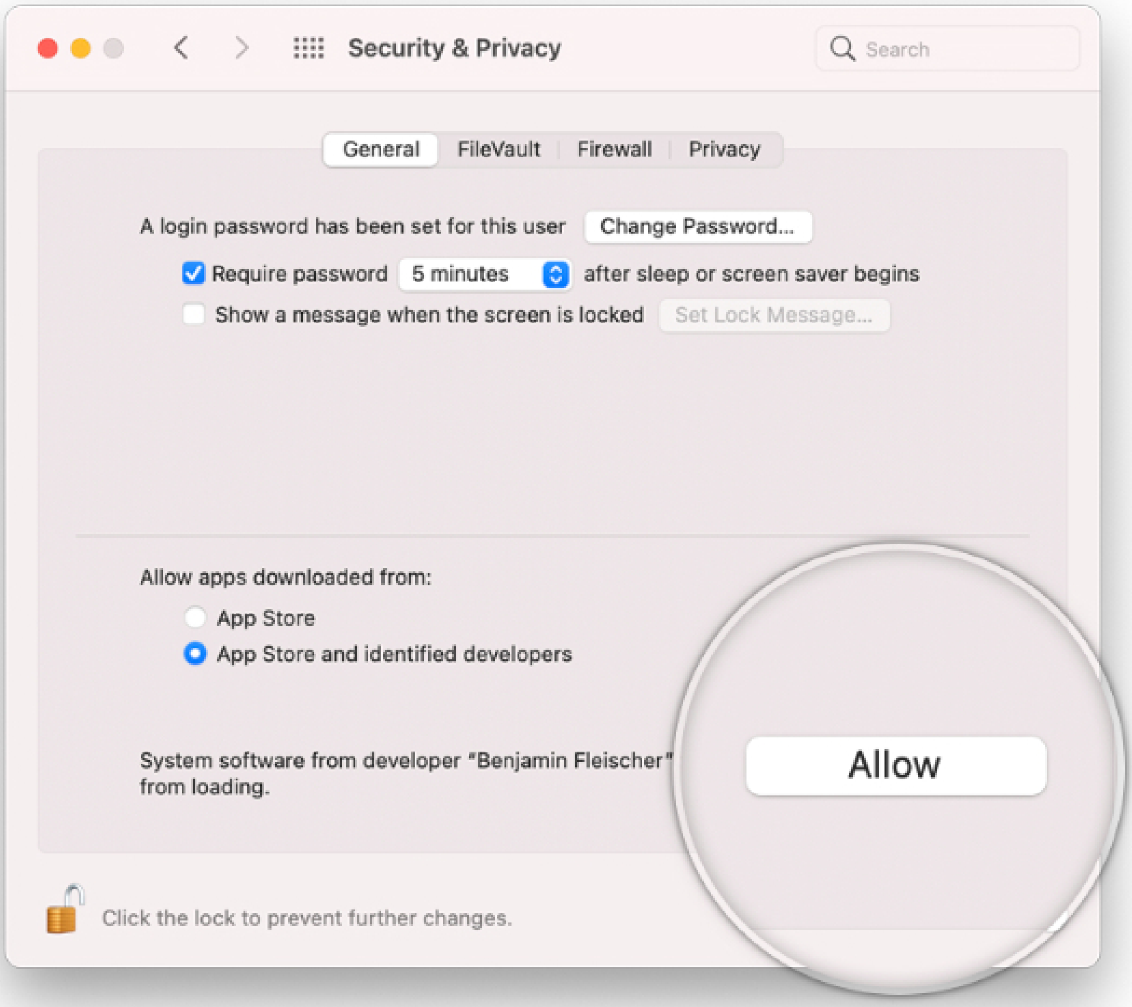


Allow Boxcryptor System Extension

> Allowing the Boxcryptor system extension is a hard requirement to use Boxcryptor and Boxcryptor will not work otherwise.

The Boxcryptor kernel extension is blocked by default and must be allowed by a user with administrator rights before it can be loaded. You will automatically be prompted to allow the Boxcryptor system extension when running for the first time if required. In this case open **System Preferences -> Security & Privacy** and follow the provided instructions.

Note: Benjamin Fleischer is the maintainer of the open source kernel extension used by Boxcryptor.



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from developer "Benjamin Fleischer" from loading.

Click the lock to prevent further changes.

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.

> 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 go to:

https://calendly.com/boxcryptor-support/disable-2fa-en

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 2.46.1667 & 2.46.1668 (2022-03-21)

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

Download v2.46.1668 for macOS 11 - 12

Download v2.46.1667 for macOS 10.15

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

Download v2.45.1655 for macOS 11 - 12

Download v2.45.1654 for macOS 10.15

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

Download v2.44.1602 for macOS 11 - 12

Download v2.44.1601 for macOS 10.15

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

Download v2.43.1465 for macOS 11 - 12

Download v2.43.1464 for macOS 10.15

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

Download v2.42.1437 for macOS 11 - 12

Download v2.42.1436 for macOS 10.15

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

Download v2.41.1308 for macOS 11 Big Sur

Download v2.41.1307 for macOS 10.14 - 10.15

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

Download v2.40.1234 for macOS 11 Big Sur

Download v2.40.1233 for macOS 10.14 - 10.15

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

Download

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

Download

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

Download

Version 2.37.1043 (2020-11-04)

- Minor bug fixes and improvements

Download

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.

Download

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

Download

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

Download

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

Download

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

Download

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

Download

Version 2.30.1004 (2019-10-07)

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

Download

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

Download

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

Download

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

Download

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)

Download

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

Download

Version 2.24.941 (2018-06-14)

- Minor bug fixes and improvements

Download

Version 2.23.939 (2018-05-24)

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

Download

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

Download

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

Download

Version 2.20.918 (2018-02-13)

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

Download

Version 2.19.907 (2017-12-13)

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

Download

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

Download

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

Download

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

Download

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

> 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

Download

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

Download

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

> 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

Download

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

Download

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

Download

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

Download

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

Download

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

Download

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

- Minor bug fixes and improvements

Download

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

Download

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

Download

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

Download

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

Download

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

Download

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)**

Download

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

Download

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

Download

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

Download

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

Download

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

Download

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.

Download

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.

Download

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.

Download

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.

Download

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.

Download

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.

Download

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

- Minor bug fixes and improvements.

Download

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

Download

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.

Download

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.

Download

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).

Download

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.

Download

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

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

Download

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.

Download

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.

Download

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

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

Download

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

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

Download

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.

Download

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.

Download

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

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

Download

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.

Download

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

Download

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

- Fixed: Issue with desktop alias creation.

Download

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

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

Download

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

Download

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

Download

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

Download

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.

Download

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.

Download

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.

Download

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

Download

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.

Download

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

Download: Download

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

Download

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

- Minor bug fixes and improvements

Download

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

- Initial Release

Download

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