Introduction

What is the Cloud?

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

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

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

What is Boxcryptor?

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

What Boxcryptor is **Not**

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

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

Quickstart

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

Install Boxcryptor

System Requirements: Requires iOS 14 or later. Boxcryptor for iOS is compatible with iPhone, iPad, and iPod touch. Please note that we do not officially support beta versions of iOS. New versions of iOS, 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, download the Boxcryptor app from the App Store.

ℹ On iOS, you do not have to install your cloud provider's app because we are able to directly connect with your cloud provider. If you have your provider's app installed, you can safely remove it after you set up Boxcryptor.

Create a Boxcryptor Account

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

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

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

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

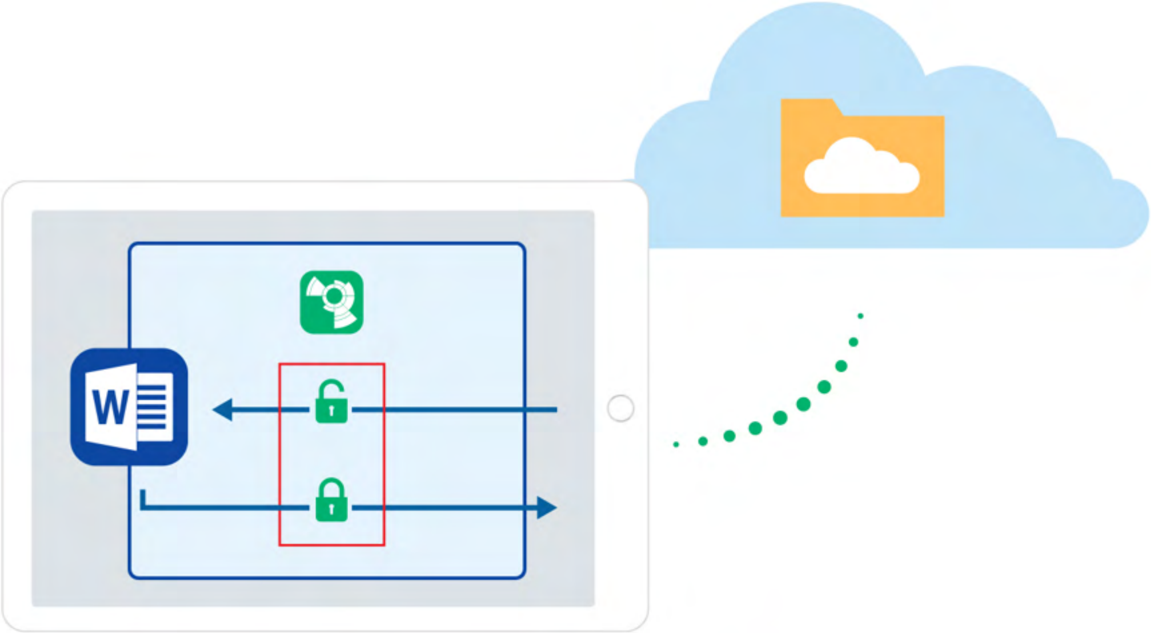
ℹ If you lose your password, your data will be lost irrevocably.

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

Discover Boxcryptor

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

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



Tags are used to show you whether a file or folder is encrypted ●.

You will be able to use Boxcryptor via the **Files app** from within other apps, such as Word or Pages.

How to Encrypt Existing Files

Encrypting existing files is not possible with Boxcryptor for iOS. Please use Boxcryptor for macOS, Boxcryptor for Windows or Boxcryptor Portable to migrate and encrypt your existing files.

Manage Clouds and Locations

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

Add Provider

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

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

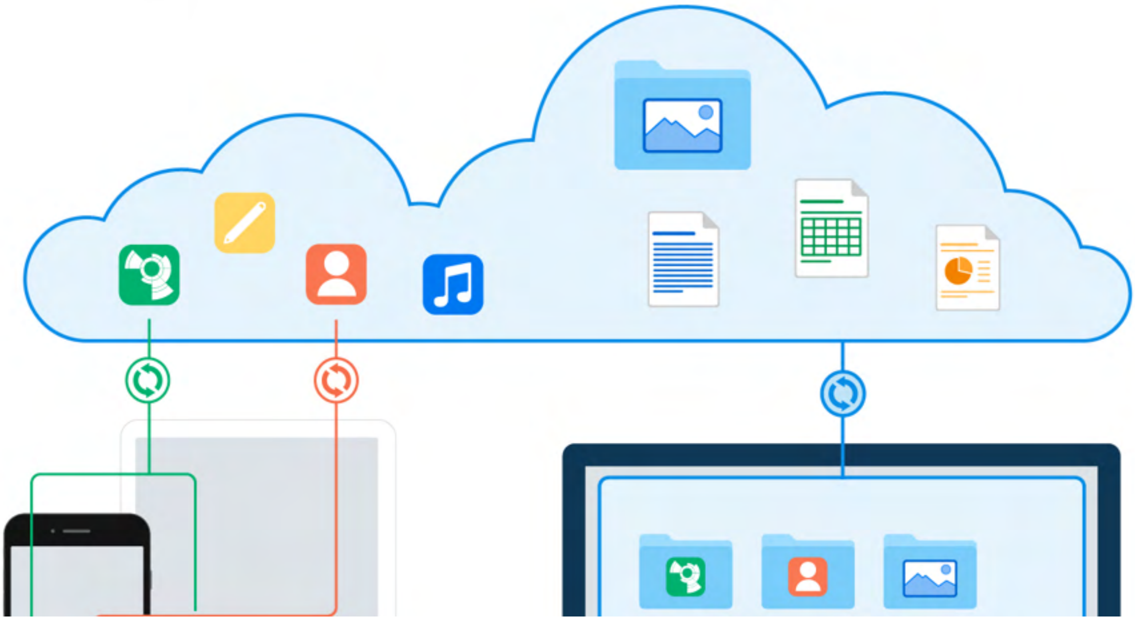
> You can also **rename** or **delete** your provider with a long press.

Google Drive

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

iCloud

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.

WebDAV Locations

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

1. Contact your cloud provider for the WebDAV credentials.

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

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

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

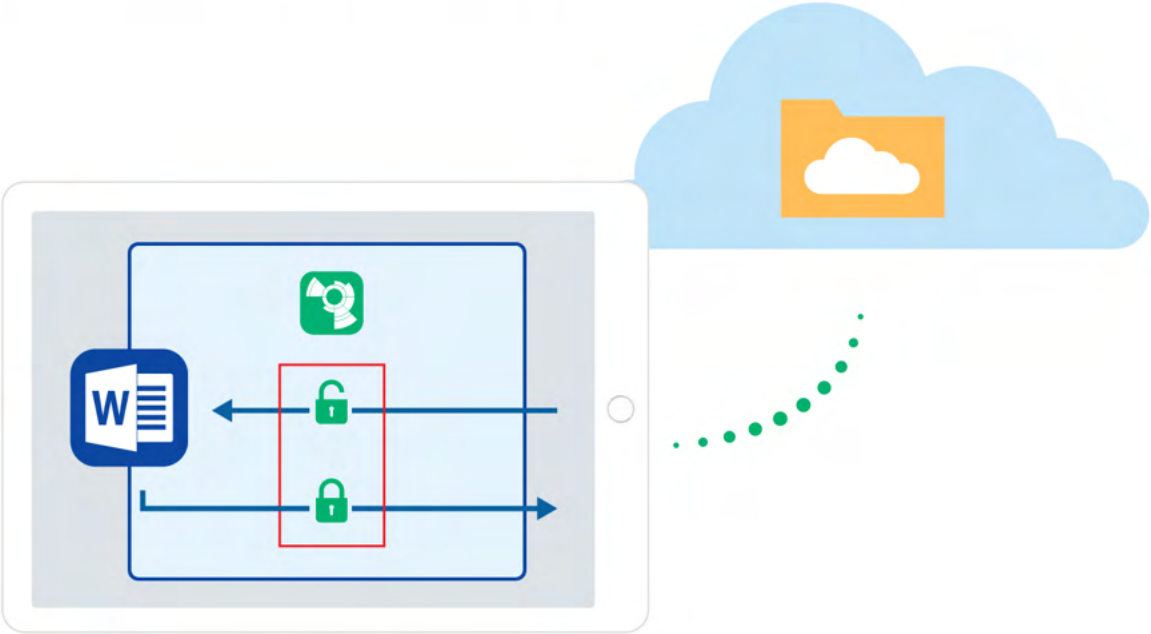
ownCloud and **nextCloud** both support WebDAV. By default, the configuration URLs are:
`https://example.com/owncloud/remote.php/webdav` *and*
`https://example.com/nextcloud/remote.php/dav/files/username/`

Work With Files

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

On-the-fly Encryption

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

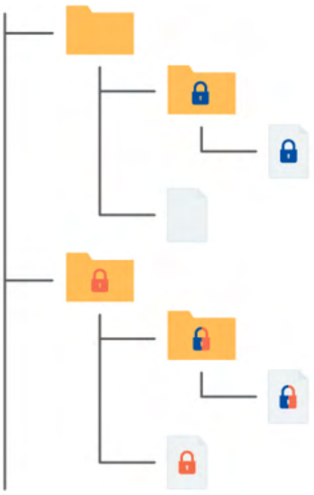


We decrypt and encrypt your files on demand: Do you want to view your content? Just tap on it and we download and decrypt your file for you. Are you finished with writing your essay? Just send it to Boxcryptor and we encrypt the file and store it into the cloud.

Encryption and Permission Hierarchy

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

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



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

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

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

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

Work With Your Files

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

The Boxcryptor **Files app integration** let you browse into folders or preview files by tapping on them. Boxcryptor will **automatically download and decrypt files** for you.

Features Within the Files App

With Boxcryptor within the Files app you can:

- Edit and save files that are encrypted with Boxcryptor
- Drag and drop files
- Execute operations on multiple items at one go
- Use advanced sorting options (Name, Date, Size, and Tags)
- See thumbnail previews for downloaded content
- Browse other cloud providers that do not have their own Files App integration

More features of the Files app can be found in Apple's own documentation.

Current Limitations

- New files and folders will inherit the encryption status of their parent location.
- New files and folders are **always encrypted**.

How to Recognize Encrypted Files

Boxcryptor allows you to have **encrypted and unencrypted** files and folders. Within the Files app, the encryption status is shown with the help of **Tags**:

- 🟢 **encrypted**
- ● **unknown**
- Without tag: **unencrypted**

> The encryption status of a folder is only determined when you browse the folder for the first time.

Encrypt Existing Files and Folders

Encrypting already existing files is currently not possible with Boxcryptor for iOS. Please use Boxcryptor for macOS, Boxcryptor for Windows or Boxcryptor Portable to migrate your existing files.

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: 恂悰挦抱砦抮殯枏瞻擟豛漢快搬濂檬浉楻挭抧柜櫸䀣.bc

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

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

To enable filename encryption globally, open the **Boxcryptor App**, navigate to **Settings** and switch on **Enable filename encryption**.

> Existing files without filename encryption will remain unchanged. Please use one of our desktop clients to activate filename encryption for your existing files.

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 a file or folder to be decrypted but synced to your cloud provider, please use Boxcryptor for macOS, Boxcryptor for Windows or Boxcryptor Portable.
- If you want to copy or move your files to another location or app, the File app has an export option to do so.

Camera Upload

The Camera Upload backs up any photo or video you take with your iPhone or iPad. All new photos or videos are saved **automatically and encrypted** to **Boxcryptor Photos** within your previously selected cloud provider.

The folder and all included files will have file name encryption turned on by default. File name encryption for Camera Upload cannot be disabled and the folder name cannot be changed due to technical reasons.

Not all cloud providers support Camera Upload because they may lack necessary write permissions.

To enable Camera Upload, follow these steps:

1. Open the **Boxcryptor App** and navigate to **Settings**.
2. Tap on **Enable Camera Upload**.
3. Allow Boxcryptor to send notifications and give it access to **all** your photos
4. Select a cloud provider you want to upload to. If you have only one compatible cloud provider added to Boxcryptor, it will be displayed and selected automatically.
5. Select if you also want to **use mobile data** for uploading photos and videos.

To disable Camera Upload tap on **Enable Camera Upload** again.

The camera upload is scheduled to run daily and will do so if the conditions are satisfied:

- correct network connection
- device charging
- sufficient available processing power

Solely iOS is responsible for triggering the camera upload and it can take up to 2-3 days even if all conditions are satisfied.

⚠ If the Boxcryptor app is closed (for example by tapping twice on the home button and swiping it away), **the camera upload will no longer work until the Boxcryptor app ist opened again**.

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

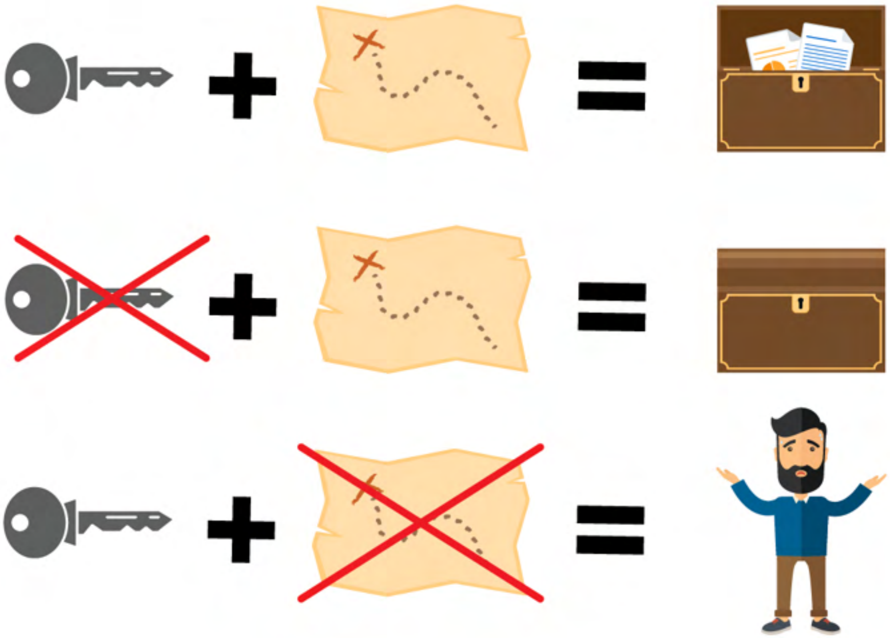
For understanding how the sharing of encrypted files works, it is helpful to understand how programs handle unencrypted and encrypted files.

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**.

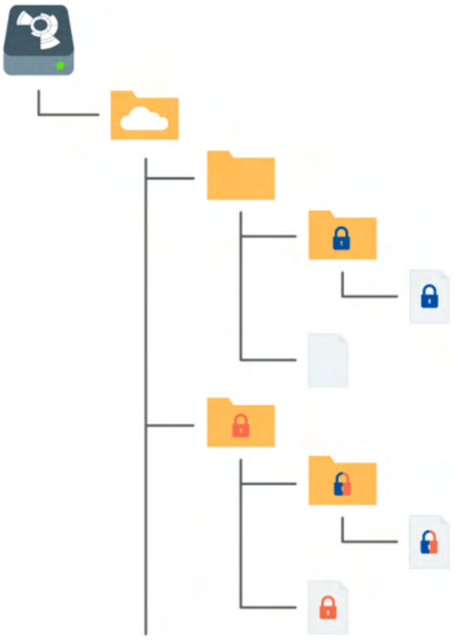
As a consequence, there are two steps necessary to share an encrypted file:

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

Managing permissions is not possible with Boxcryptor for iOS. Please use Boxcryptor for macOS or Boxcryptor for Windows to manage permissions.

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. Whisply is not integrated into Boxcryptor for iOS. You can use the browser version of Whisply to share files or folders with non-Boxcryptor users.

Manage Groups

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

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

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

Benefits of Groups

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

The benefits of groups are:

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

Settings

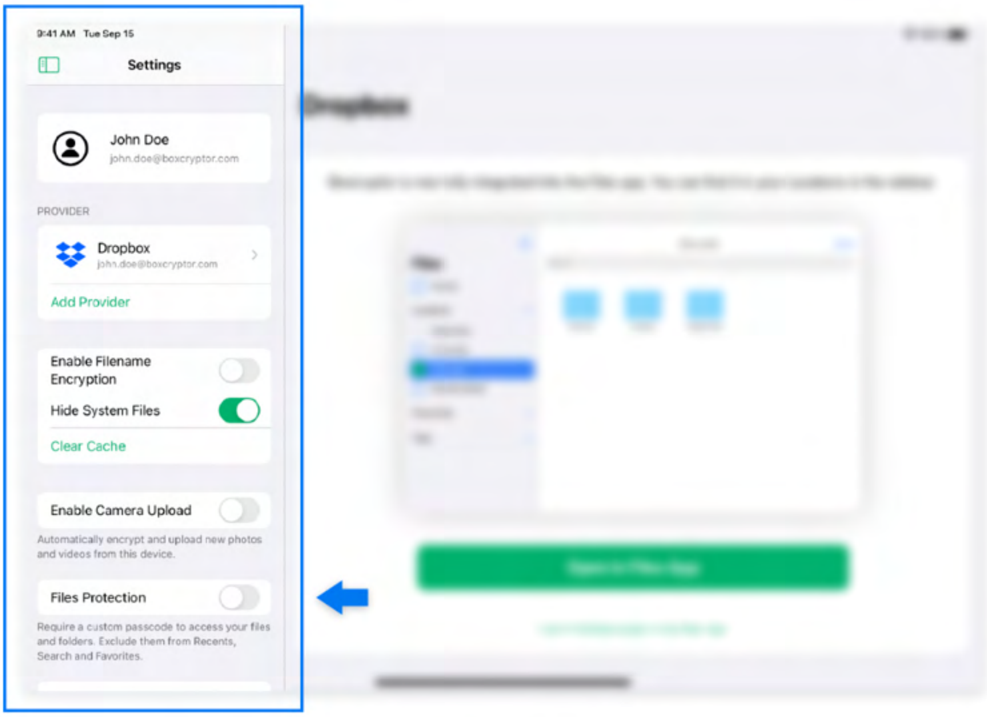
App Protection

In Boxcryptor for iOS, App Protection was replaced by **Files Protection**. Files Protection prevents unauthorized access to **files and folders saved to the Boxcryptor location** within the Files app. The Boxcryptor app itself does not contain files or folders anymore. To use this feature, activate the "Files Protection" switch in your Boxcryptor app and set your personal, six-digit **Boxcryptor passcode**. The passcode is **independent from your device code and Boxcryptor password**.

Further Setting Options:

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

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



9:41 AM Tue Sep 15

Settings

John Doe
john.doe@boxcryptor.com

PROVIDER

Dropbox
john.doe@boxcryptor.com

Add Provider

Enable Filename Encryption ○

Hide System Files ●

Clear Cache

Enable Camera Upload ○

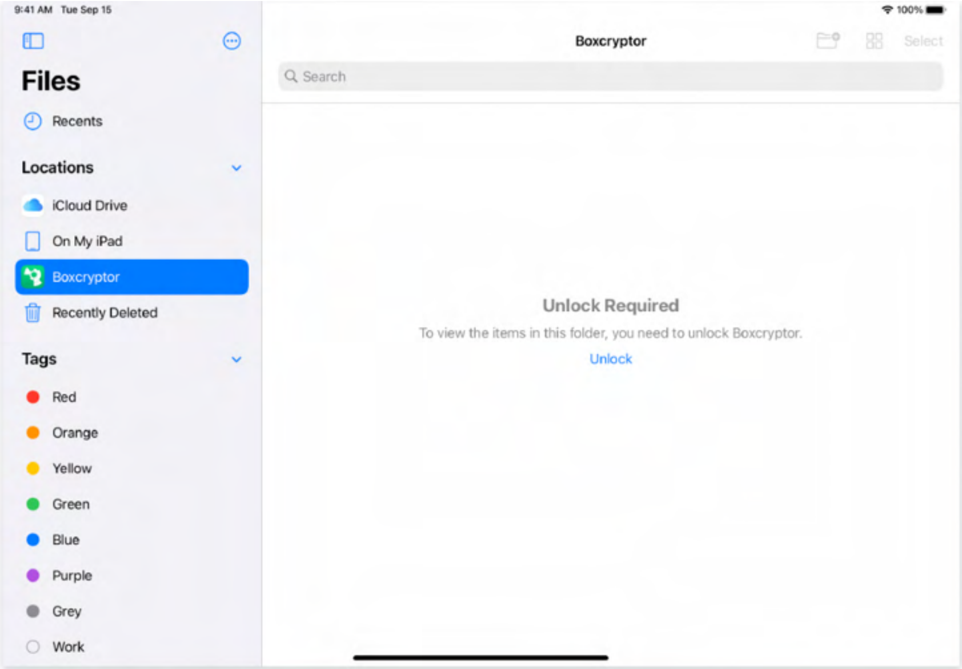
Automatically encrypt and upload new photos and videos from this device.

Files Protection ○

Require a custom passcode to access your files and folders. Exclude them from Recents, Search and Favorites.

Setting up Files Protection, Step 1: Toggle switch inside the **Boxcryptor app**.

If you now open the Boxcryptor location in the Files app, you will be asked to unlock access with your new Boxcryptor passcode first.



Unlock Required

To view the items in this folder, you need to unlock Boxcryptor.

Unlock

Boxcryptor Files Protection: Locked **Files app location**.

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

Technical Limitations

- If you're using **Save to Files** in the locked state, the Boxcryptor location will we be shown but disabled. You need to open the Boxcryptor app and unlock it again.
- Automatic, time based locking is not available anymore as we cannot remove locations without user interaction. To protect your files and folders locally, you need to lock them manually in the Boxcryptor app -> **Home** -> **Lock Now**. A notification will remind you, that your files and folders are unprotected.

Boxcryptor Settings

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

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

- Enable Filename Encryption,
- **Hide System Files**,
- **Clear Cache**,
- Set up the Camera-Upload,
- Set up Files Protection
- and **Sign Out** of your Boxcryptor account to reset the app to factory defaults.

Files App Documentation

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

‹ PREVIOUS

NEXT ›

Boxcryptor Account

Manage Your Account

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

Restoring Your Password

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

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

You can reset your account here.

Manage Your Devices and Sessions

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

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

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

Export Your Keys

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

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

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

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

Local Account

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

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

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

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

How to export a Key File

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

How to Open an Existing Key File

1. Send the key file to your device, for example via email or AirDrop.
2. Select the key file and send it to the Boxcryptor app.
3. Enter your password to sign in to 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**.

> 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:

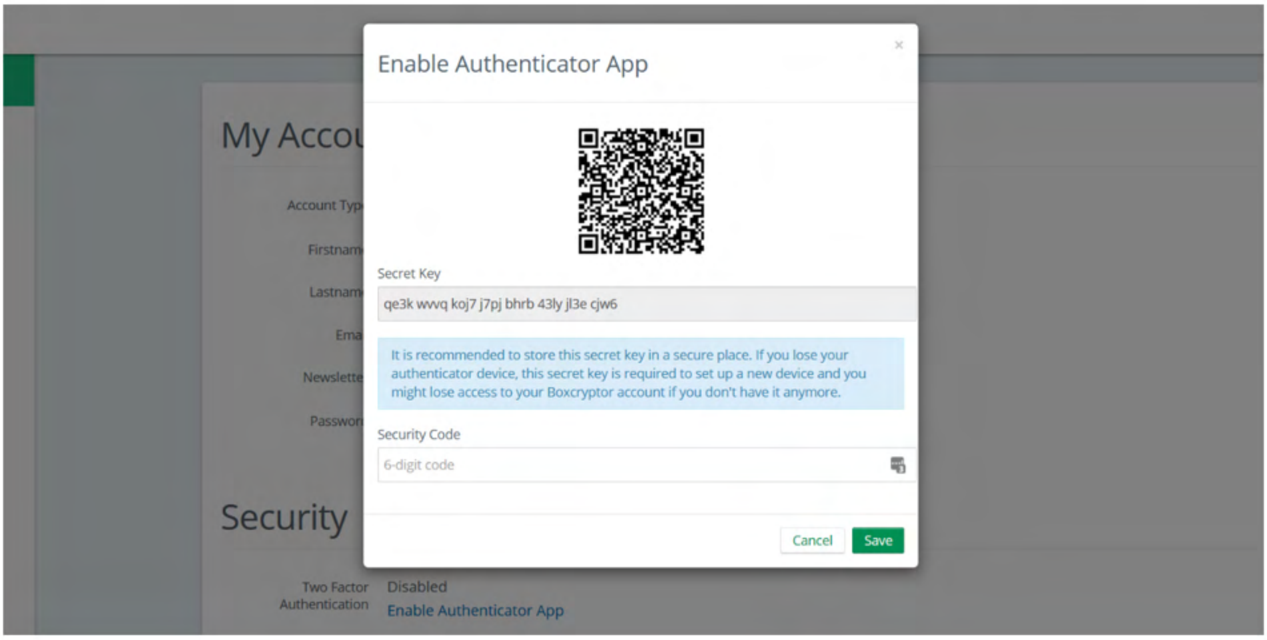
1. Sign in to boxcryptor.com.
2. Navigate to **Security**.
3. Click on **Two-factor Authentication -> Authenticator App**.
4. Scan the QR code with your Authenticator App. Copy the **Secret Key** and store it in a secure place.
5. To complete the setup, enter the 6-digit code from your authenticator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

[redacted]

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

Enable Authenticator App

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

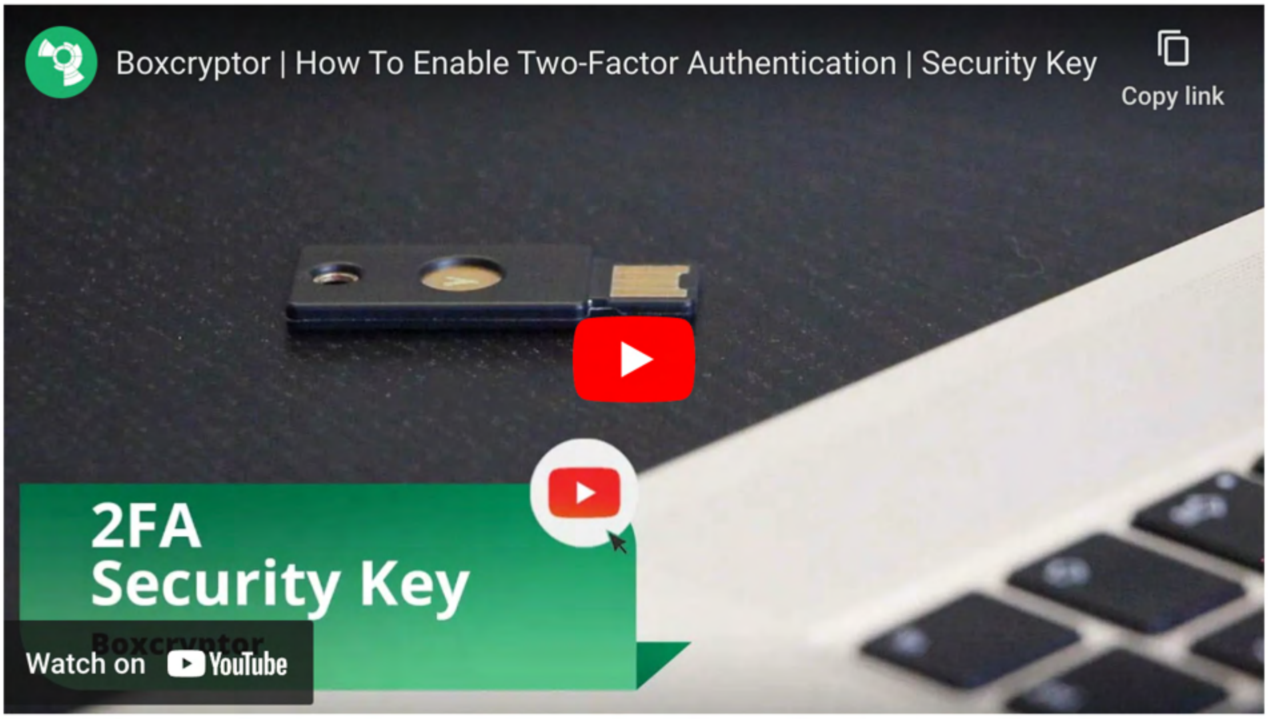
Security Keys

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

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

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

Read more about security tokens on our blog


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

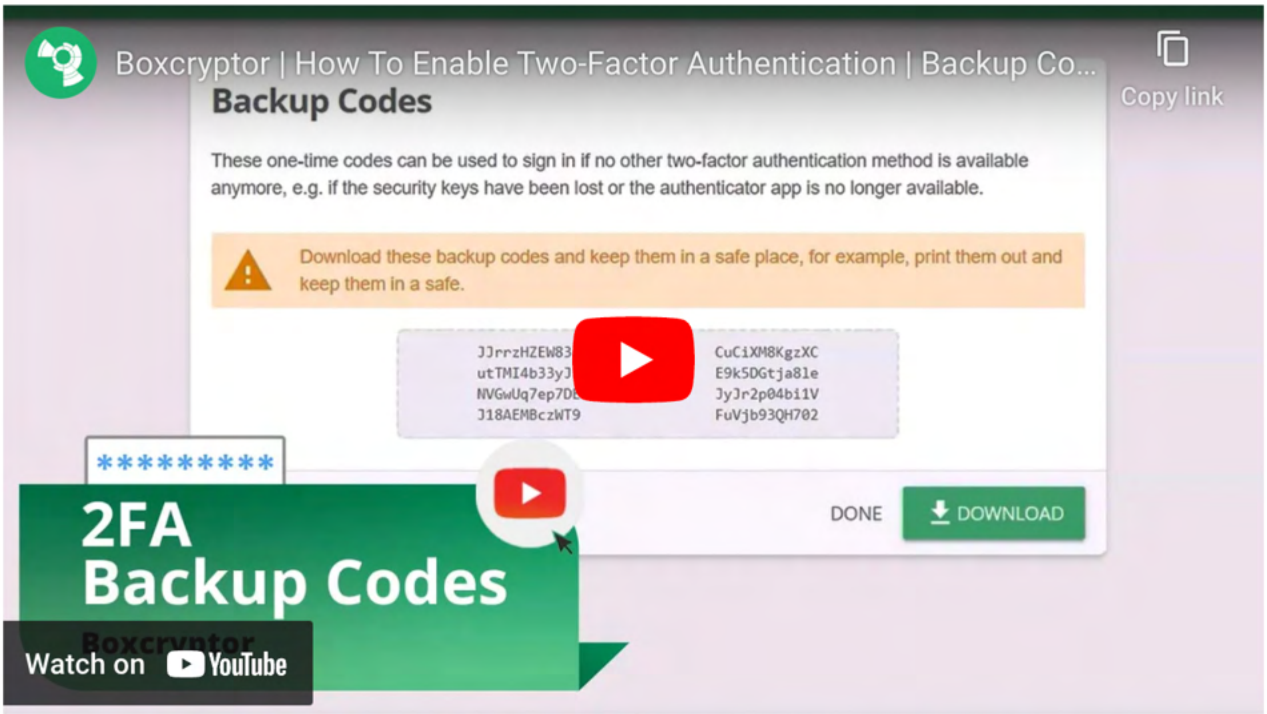
To prevent a lockout we recommend registering two security keys. Use one regularly, keep the other one as backup in case that you loose the first one. Alternatively, you can set up TOTP as a second factor backup.

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

Backup Codes

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

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



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

Backup Codes

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

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

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

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

2FA and the Protection feature

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

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

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

FAQ & Troubleshooting

Off-Migration Guide: Decrypt all Boxcryptor encrypted files

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

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

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

Migration Tips For Organizations

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

To decrypt your files, we recommend using our Desktop applications Boxcryptor for Windows or Boxcryptor for macOS.

If you cannot access your files on these platforms, you can also copy and paste your encrypted files and folders to your iPhone or iPad using the `Files-app`.

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

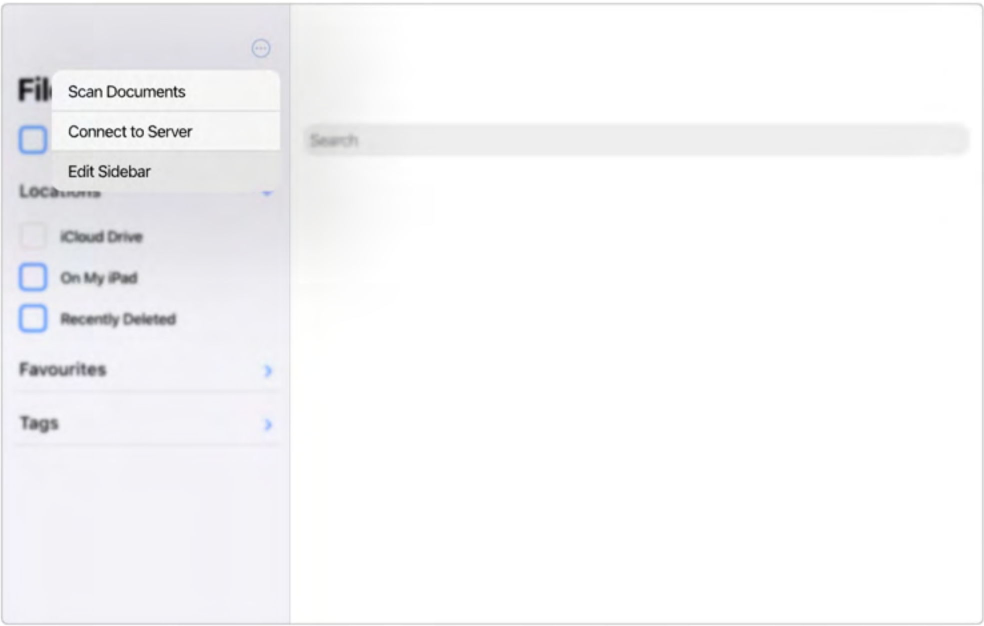
When these files are available, you will always be able to access your encrypted files on your own on any supported operating system - without any connection to any server. The exported key file contains all encryption keys associated with your Boxcryptor account. *Important:* As new keys might be added 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.

Boxcryptor does not show up in Files app

In some cases, Boxcryptor is not shown directly in the Files app after installation.



You may have to edit your Locations list to activate your Boxcryptor Location. Press ⋯ -> **Edit Sidebar** -> **Toggle on the Boxcryptor Location**.

Use self-signed Certificates for Cloud Provider

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

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

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

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

I Cannot Move a File to an Encrypted Folder

Moving files between differently encrypted folders or into a new encrypted folder always requires encrypting the files with the new folder key. Hence, Boxcryptor has to download the item, decrypt, encrypt, and upload the item again. This would present an obvious strain on your bandwidth. Since users might not expect this much data usage for a simple move/copy operation, we decided to disable the option to move and copy between encrypted folders.

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.

Boxcryptor Classic for iOS is not available on in the App Store anymore.

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.

What is a FolderKey.bch and a .bclink file

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

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

Does it Leak Sensitive Information?

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

What Happens When I Lose it?

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

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

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

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

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

Does it Leak Sensitive Information? Can I delete it?

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

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

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

Ways to recover access to your account:

Re-apply the secret key from your initial setup

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

For reference, the secret key looks similar to:

> mzwe wocd mj3d qr3f njjw g2cm grqw cvli

Use a device code

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

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

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

Use a backup code

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

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

None of the above methods apply

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

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

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

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

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

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

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

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

Invalid Authenticator App Codes

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

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

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

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

Why Is Boxcryptor “Files App First”?

With iOS 11, Apple introduced the Files app as the central hub and designated way to work with files on iPhones and iPads in 2021. Besides the default storage locations iCloud and "On my device", apps like Boxcryptor can integrate with the Files app and provide their own files and folders. At the same time, other apps can integrate the Files app in order to seamlessly work with exactly those files.

The Files app is a huge improvement for workflows spanning multiple apps to get your work done. Our mission and promise at Boxcryptor is and has always been to secure your files stored in the cloud.

> Our mission is to become the service of choice for everyone who wants to secure files in the cloud. Today, cloud computing is part of our everyday lives and it is continuously changing and evolving. The influence that cloud computing has on our personal and business lives will have a lasting impact on our world. Therefore, data security in the cloud is of highest priority. Personal and sensitive information are valuable property that must be protected – today and always. Boxcryptor was born inspired by our passion for cloud computing security and our wish to find new solutions to make our lives a little easier and more secure. As we grow, we will continue to protect information across devices in the cloud and to develop services and solutions as needs and wants evolve.

This mission is our guideline when developing Boxcryptor now and in the future. *Files app first* is an important step on this journey and ensures that we continue to meet our customer's requirements in 2021 and beyond. You can learn more about the advantages of the Files app here.

Why Did You Remove Your Own File Browser?

On one hand, developing and maintaining your own files browser including all bells and whistles requires a huge effort, on the other hand it can never match the experience Apple is able to provide with the Files app due to its central and deep integration in iOS and other apps.

Focusing on the Files app integration allows us to provide a more clear user experience by having a single place to work with your encrypted files and also to opimize our development resources around our core value proposition: The best end-to-end encryption solution for cloud storages.

I Don’t Trust Apple, iOS or the Files App

Apple owns the hardware, the operating system, and all core apps running on your iPhone or iPad. It is impossible to develop a third party iPhone or iPad app which can protect data against Apple as an attack vector.

If you do not trust Apple, iOS or the Files app, the only real solution is not to use an Apple device. You should only use devices and operating systems which have your trust.

App security always relies on operating system security and operating system security always relies on hardware security. Thus, trust is inherited: Hardware must be trusted to trust the operating system. The operating system must be trusted to trust an app. If trust for the hardware or operating system are missing, this trust can never be restored by an app.

The new Boxcryptor app is as secure as the old one was. Even if you disabled the Files app integration in the old app, Boxcryptor – just like every app - always used functionality provided by iOS, e.g. to perform the actual encryption and decryption or to preview files within the Boxcryptor app. Files in the Boxcryptor app have always been exposed to Apple's software and hardware - regardless if the Files app integration was used or not.

Just like iOS, the Files app adheres to the highest standards for privacy and data security found in the industry. Other apps can only access files in the Files app if you explicitly opened a file. **It is not possible that other apps secretly access your encrypted files in Boxcryptor via the Files app behind your back.** You can learn more about the security of Apple platforms here.

I Don’t Trust Other Apps

By default, the Files app automatically opens a file in another app if it supports the file type. For example, Word documents will automatically open in the Word or Office app if it is installed.

If you have apps installed which you don't trust, the only real solution is to uninstall them. You should only install and use apps which have your trust.

If you do not want that a specific file opens in another app, you can use the Quick Look feature of the Files app to preview a file directly in the Files app. You can learn more about it here.

About

Maintenance Window

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

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

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

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

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

Changelog

Version 3.24 (2022-11-17)

- Fixed bug when adding cloud storage provider
- Fixed bug when unlock the Files Protection

Version 3.23 (2022-11-11)

- Fixed rename of a file name encrypted folder leads to access denied error
- Fixed files remain in waiting state while downloading or uploading
- Besides recent sites SharePoint now lists all sites the user has access to instead of only followed sites
- Minor bugfixes and improvements

Version 3.22 (2022-10-19)

- Fixed editing of Office files
- Improved SharePoint site and MS Teams Channel listing
- Improved local file cache cleanup
- Minor bugfixes and improvements

Version 3.21 (2022-09-28)

- Fixed large file uploads and downloads on iCloud
- Minor bugfixes and improvements

Version 3.20 (2022-08-30)

- Minor bugfixes and improvements

Version 3.19 (2022-08-01)

- Files Protection now removes Boxcryptor locations in Files App
- Improved Files Protection Manual Lock process
- Improved disk space consumption
- Fixed Clear Cache Button did not work properly
- Fixed bug when opening files on Strato HiDrive
- Removed Files Protection Auto-Lock
- Added device code to recover Account Access if Second Factor (2FA) is Lost
- Minor bugfixes and improvements

Version 3.18 (2022-06-08)

- Added LeitzCloud to our supported cloud storage provider list
- Minor bugfixes and improvements

Version 3.17 (2022-04-04)

- Fixed Google Drive deleted Shortcuts handling
- Fixed Share to Boxcryptor with enabled Files Protection
- Minor bugfixes and improvements

Version 3.16 (2022-03-21)

- Support Google Drive Shortcuts
- Fixed MagentaCLOUD authentication issues
- Fixed MagentaCLOUD connection issues
- Fixed usage of multiple Nextclouds at the same time
- Improved OneDrive error handling
- Minor bugfixes and improvements

Version 3.15 (2022-02-07)

- Added: Tabs for improved usability
- Improved: Each provider now has its own Boxcryptor location in the Files app
- Fixed: Old shared files cannot be decrypted

Version 3.14 (2021-12-04)

- Support new MagentaCLOUD

Version 3.13 (2021-12-02)

- Support new MagentaCLOUD

Version 3.12 (2021-10-05)

- Fixed: Boxcryptor sign-in after device change

Version 3.11 (2021-09-27)

- Fixed: Camera Upload may not start uploading

Version 3.10 (2021-09-20)

- iOS 15 Support
- Added Files Protection

Version 3.09 (2021-08-18)

- Minor bugfixes and improvements

Version 3.08 (2021-05-27)

- Minor bugfixes and improvements

Version 3.07 (2021-05-13)

- Minor bugfixes and improvements

Version 3.06 (2021-05-09)

- Minor bugfixes and improvements

Version 3.05 (2021-05-06)

- Minor bugfixes and improvements

Version 3.04 (2021-05-03)

- Minor bugfixes and improvements

Version 3.03 (2021-04-28)

- Files App First Find all your encrypted files in the Files App and only there.
- Security Keys Sign in with your security key for additional account protection.
- Microsoft Teams Work with encrypted files stored in Microsoft Teams.
- App Protection Removed Access to files in the Files app cannot be additionally protected.

Version 2.51.901 (2021-01-11)

- Minor bugfixes and improvements

Version 2.50.889 (2020-10-29)

- Minor bugfixes and improvements

Version 2.49.887 (2020-09-25)

- Minor bugfixes and improvements

Version 2.48.869 (2020-09-16)

- Official iOS 14 Support
- You can now add up to 5 photos at once
- Improved iCloud performance
- Improved Dropbox listing
- Minor bugfixes and improvements

Version 2.47.865 (2020-05-08)

- Minor bugfixes and improvements

Version 2.46.861 (2020-04-14)

- Added LeitzCloud to our supported cloud storage provider list
- Fixed Camera Upload uploading already uploaded photos.
- Minor bugfixes and improvements

Version 2.45.857 (2020-02-04)

- Minor bugfixes and improvements

Version 2.44.853 (2019-12-11)

- Minor bugfixes and improvements

Version 2.43.851 (2019-11-18)

- Minor bugfixes and improvements

Version 2.42.847 (2019-09-27)

- Minor bugfixes and improvements

Version 2.41.846 (2019-09-19)

- Official iOS 13 Support
- Beautiful new user interface
- Dark Mode support
- Minor bugfixes and improvements

Version 2.40.840 (2019-08-26)

- Fixed: Provider Box sometimes asks user for Credentials
- Improved: Connection to Provider HubiC
- Improved: Connection via WebDAV
- Removed: Outdated Cloud-Provider GrauData
- Minor bugfixes and improvements

Version 2.39.836 (2019-07-22)

- Minor bugfixes and improvements

Version 2.38.832 (2019-06-09)

- Benvenuto, bienvenida & bienvenue - Added Italian, Spanish and French localization
- Added: Provider Wasabi
- Added: Select any document library within a SharePoint site
- Improved: Connection to AmazonS3
- Improved: Connection to Mail.ru
- Improved: Connection to SugarSync
- Improved: Connection to Egnyte
- Improved: iOS PasswordManager support - Passwords can now be autofilled
- Fixed: Some files in iCloud can not be opened
- Fixed: Some files can not be added to Boxcryptor
- Fixed: Externally updated files sometimes not updated
- Minor bugfixes and improvements

Version 2.37.826 (2019-01-16)

- Minor bugfixes and improvements

Version 2.36.824 (2018-12-14)

- Improved: Reduced memory consumption
- Improved: Connection to Amazon Cloud Drive
- Improved: Connection to Yandex Disk
- Improved: Connection to iCloud
- Improved: Connection to Orange Cloud
- Fixed: Box sometimes displayed wrong dates
- Fixed: Files did not update on Favorites tab
- Minor bugfixes and improvements

Version 2.35.820 (2018-11-12)

- Improved: App start time
- Fixed: Sign in without internet connection does not work
- Added: Strato HiDrive special character filename support

Version 2.34.818 (2018-10-19)

- Improved: Files App integration
- Improved: Connection to Provider Box
- Improved: Connection to Provider MagentaCloud
- Improved: Connection to Provider HiDrive
- Minor bugfixes and improvements

Version 2.33.815 (2018-10-16)

- Minor bugfixes and improvements

Version 2.32.807 (2018-09-26)

- Minor bugfixes and improvements

Version 2.31.804 (2018-09-24)

- Improved: Connection to Provider GoogleDrive
- Improved: Connection to Provider OneDrive
- Fixed: OneDrive login not possible on small devices
- Minor bugfixes and improvements

Version 2.30.799 (2018-07-23)

- Improved: Files App Integration
- Fixed: Discovered directory handled as being unencrypted
- Fixed: Activities tab not cleaned at sign out
- Minor bugfixes and improvements

Version 2.29.797 (2018-07-16)

- Improved: Dropbox connection
- Fixed: FaceID fails on second attempt
- Fixed: WebDav login sometimes fails
- Minor bugfixes and improvements

Version 2.28.791 (2018-05-24)

- Updated: Privacy Policy

Version 2.27.790 (2018-05-17)

- Added: Russian localization
- Fix: App might signout user when adding a provider
- Minor bugfixes and improvements

Version 2.26.783 (2018-03-26)

- New: ownCloud and Nextcloud support
- Improved: 'Save to Boxcryptor' compatibility
- Added: Dropbox Team Spaces

Version 2.25.780 (2018-02-12)

- Extended WebDAV support
- Added Google Drive 'Shared with me' Directory
- Improved OneDrive Germany support
- Enhanced Spark Mail support
- Added Provider SharePoint 2013
- Minor bug fixes and improvements

Version 2.24.774 (2017-12-20)

- Minor bug fixes and improvements

Version 2.23.771 (2017-12-7)

- New Feature: German translation
- New Feature: Sharepoint site entry form
- Fixed: WebDAV Encoding
- Fixed: OneDrive Shared Directories did not update
- Fixed: Directories with dots were displayed as packages in Files app
- Minor bug fixes and improvements

Version 2.22.769 (2017-11-20)

- Fixes white screen after tour
- Improves Camera Upload stability

Version 2.21.764 (2017-11-13)

- Fixes to Camera upload
- Files App stability
- iCloud performance improvements
- "Shared With Me" Directory for OneDrive
- Hubic showed empty directories
- Small bug fixes

Version 2.20.756 (2017-09-29)

- Fixed: Downloading/Uploading failed in background configuration
- Fixed: Saving to Photos did not ask for permission
- Fixed: Create Directory did not work

Version 2.19.752 (2017-09-22)

- Fixed: Crashes for some devices
- Fixed: "Save to Boxcryptor" dialog did not display

Version 2.18.743 (2017-09-19)

- Files App Integration
- Fixed: WebDAV with HTTP
- Fixed: Camera Upload for videos

Version 2.17.726 (2017-09-12)

- Fixed: Blank screen on iOS 11 Beta
- Fixed: Camera Upload sometimes crashed
- Small bug fixes

Version 2.16.725 (2017-09-04)

- New Feature: Camera Upload: Automatically upload your photos and videos
- Fixed: Word zero KB files
- Fixed: Livedrive filename encryption
- Fixed: Working with Favorites tab
- Fixed: WebDAV multi-user issues

- Fixed: OneDrive shows wrong modified/created date

Version 2.15.722 (2017-08-15)

- Fixed: Crash for local accounts when policies were set.
- Fixed: Upload issue for Dropbox

Version 2.14.721 (2017-08-09)

- Improved: Faster access to large directories in OneDrive
- Fixed: Bug on OneDrive for large document uploads
- Various other bug fixes and improvements

Version 2.13.717 (2017-07-20)

- New: Create folder while choosing a place for an upload
- New: Google Drive Team Drives support
- Various other bug fixes and improvements

Version 2.12.715 (2017-07-10)

- Small Bugfixes

Version 2.11.711 (2017-06-26)

- New: Authentication window redesign
- New OneDrive Sign Up
- Small Bug fixes

Version 2.10.708 (2017-06-21)

- Improved: Extension access time and fault tolerance
- New: Allows working with files while offline
- Fixed: Issue of background upload finish
- Minor bug fixes and improvements to extension

Version 2.8.696 (2017-05-15)

- Minor bug fixes and improvements to local account

Version 2.7.693 (2017-05-02)

- Minor bug fixes and improvements

Version 2.7.690 (2017-03-27)

- New Provider: Orange
- New Provider: Mail.ru Hotbox
- Bugfix for Amazon S3

Version 2.7.686 (2017-03-15)

- New Feature: Highlight your favourite files

- New Feature: “Save to Boxcryptor” – App extension which allows uploading multiple files from other apps.
- New Feature: “Display Password”-option during sign in
- New Provider: HubiC
- New Provider: Magenta

Version 2.7.684 (2017-01-19)

- Fixed bug with local account

Version 2.7.681 (2016-12-21)

- New Icons and UI Improvements
- Photos taken with Boxcryptor are compressed to 80% quality.

Version 2.7.679 (2016-12-12)

- Improved: A share menu is displayed in case a file can't be previewed
- Small bug fixes for iOS 9 and Document Extension
- Various stability improvements

Version 2.7.678 (2016-12-07)

- Major performance and stability improvements
- New: Search in folders
- New: Support for SharePoint Online
- New: Take photos directly within the Boxcryptor app
- Improved: Display of recent activities
- Improved: Open and edit files in third party apps
- Improved: Yandex support (Please re-add your account)
- Various other bug fixes and improvements

Version 2.6.444 (2016-10-20)

- N/A

Version 2.5.439 (2016-09-28)

- N/A

Version 2.5.435 (2016-09-26)

- N/A

Version 2.5.434 (2016-09-12)

- N/A

Version 2.5.433 (2016-05-27)

- N/A

Version 2.5.431 (2016-05-17)

- N/A

Version 2.5.430 (2016-05-10)

- N/A

Version 2.4.401 (2015-04-07)

- N/A

Version 2.3.401 (2014-04-09)

- N/A

Version 2.2.405 (2014-03-11)

- N/A

Version 2.2.403 (2014-02-20)

- 64bit support on newer iPhones & iPads
- Fixed: Box connection settings

Version 2.2.402 (2013-12-05)

- Fixed: crash on start-up when connected to SkyDrive

Version 2.2.401 (2013-12-01)

- Fixed: crash on start-up after update, when connected to SkyDrive
- Fixed: crash when trying to use a newly imported KeyFile

Version 2.2.400 (2013-11-25)

- Local Accounts
- Create new accounts
- iOS 7 UI
- Support for Cloudme & GRAU DATA providers
- Fixes for SkyDrive, LiveDrive
- Various fixes and improvements

Version 2.1.1 (2013-09-02)

- Fixed: "Infinite Unlocking" issue
- Fixed: uploads from FileDrop
- Fixed: wrong handling of decrypted files which can't be viewed in the builtin previewer
- Other minor fixes and improvements

Version 2.1 (2013-08-14)

- (Beta) Encrypt & upload files (including photos and videos from the Photo Library)

- FileDrop, a local folder where you can store files (encrypted and plain) that are opened from other applications.
- Improved log in handling and session restore
- Option to enable/disable automatic log in
- Option to enable/disable filename encryption
- Improved "Add new Provider"
- File browser shows all files: Non-encrypted files have a black font color and encrypted files have a green font color.
- Improved "User Account Info"
- Fixed: Crash on log in with new accounts
- Fixed: Various WebDAV issues
- Fixed: SugarSync & Yandex Disk log in issues

Version 2.0.1 (2013-06-11)

- Improved: Performance

Version 2.0 (2013-05-31)

- Initial Release

Network Access

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

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

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

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

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

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

Open Source Licenses

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

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