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 Android 6.0 or later. Boxcryptor for Android is compatible with smartphones and tablet devices.

To install Boxcryptor, download the Boxcryptor app from the Google Play Store.

> ℹ On Android, 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.

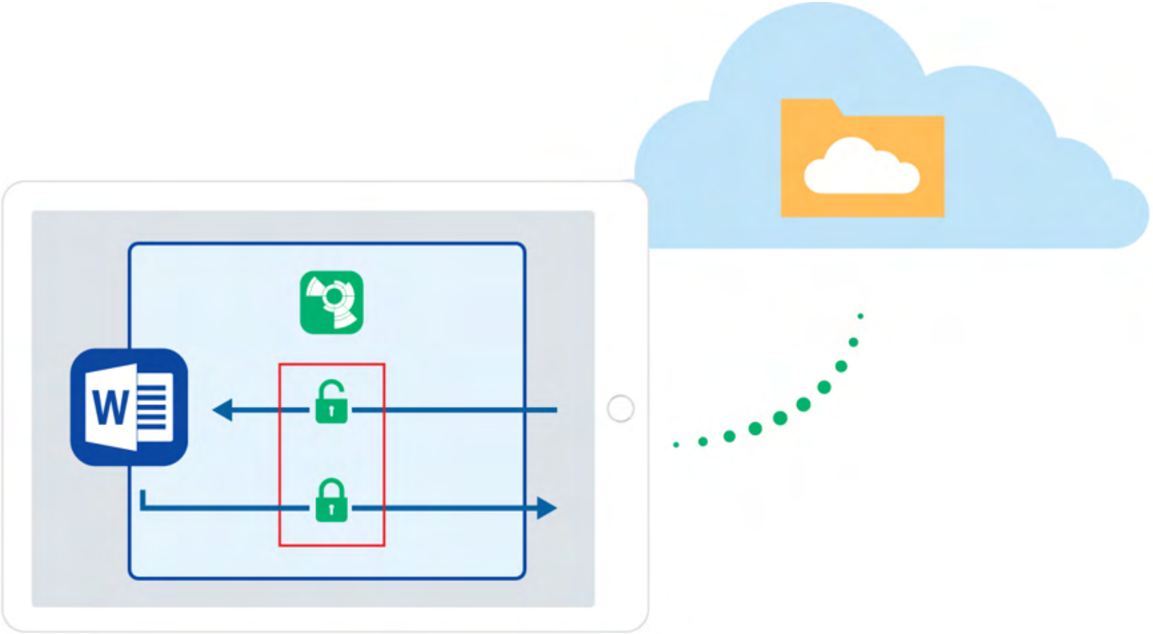
Create a password that you can remember, or store the password in a secure place, for example a password manager. Boxcryptor is a zero knowledge encryption software, therefore we **cannot** restore your password.

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

Discover Boxcryptor

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

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



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

You will be able to use Boxcryptor directly from within other apps, such as Word. For instance, if you want to edit a Word file, open Word → select **Open other documents** on the **Open** tab, → **Browser** → ☰ → select **Boxcryptor**.

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 app**.
2. Open your cloud provider in the Boxcryptor app.
3. Tap on ⊕ → **new folder**.
4. Enter a name for the new folder. The encryption option is pre-selected for you.
5. Upload files or photos to the folder. All files will be encrypted automatically.

How to Encrypt Existing Files

Encrypting existing files is currently not possible with Boxcryptor for Android. Please use Boxcryptor for Windows, Boxcryptor for macOS or Boxcryptor Portable to migrate 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 Android, 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. Tap on ☰.
2. Tap on **Settings** and **Manage Locations**.
3. In your Provider Overview tap on the **plus sign in the bottom right corner**.
4. Now **select your provider** and enter your provider's credentials to connect it to Boxcryptor.

Google Drive

Boxcryptor gives you access to files stored in Google Drive's **My Drive**. Additional folders backed up via **My Computer** are *not* available.

Custom Locations

Boxcryptor supports adding folders on your SD card or your local storage as **Local Storage** provider:

1. Tap on ☰.
2. Tap on **Settings** and **Manage Locations**.
3. In your Provider Overview tap on the **plus sign in the bottom right corner**.
4. Tap on **Local Storage** and choose your own, customized location.

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.

2. Tap on ☰.
3. Tap on **Settings** and **Manage Locations**.
4. In your Provider Overview tap on the **plus sign in the bottom right corner**.

5. Tap on **WebDAV Advanced** and enter your provider's credentials to connect it with Boxcryptor.

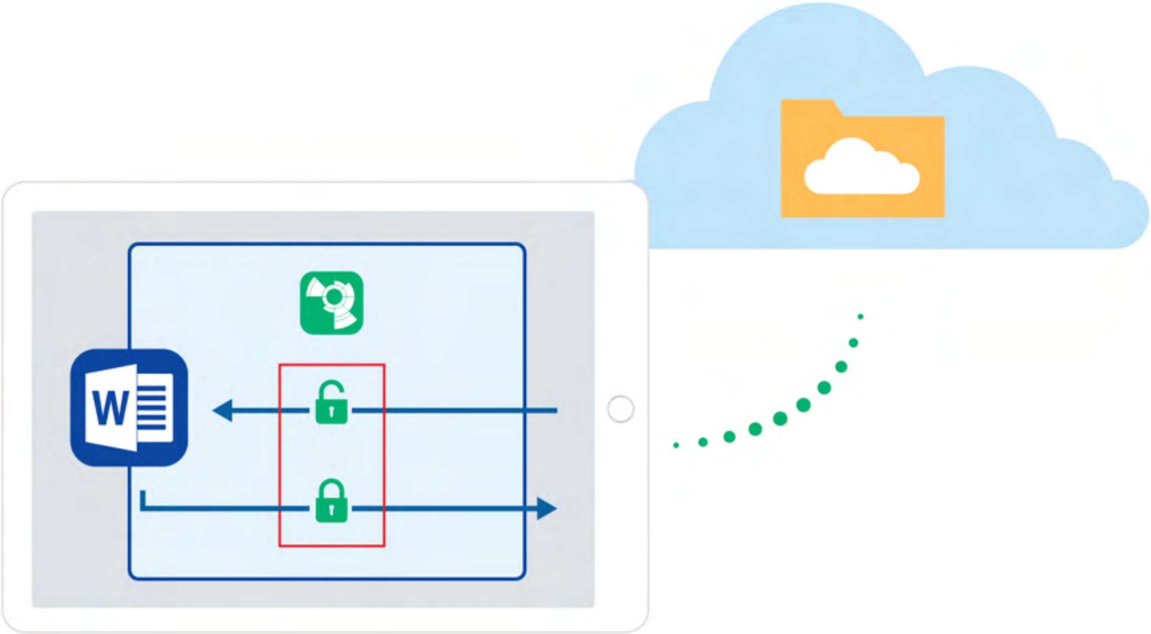
ⓘ ownCloud and nextCloud both support WebDAV. By default, the configuration urls are: `https://example.com/owncloud/remote.php/webdav` *and* `https://example.com/nextcloud/remote.php/dav/files/username/`

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.

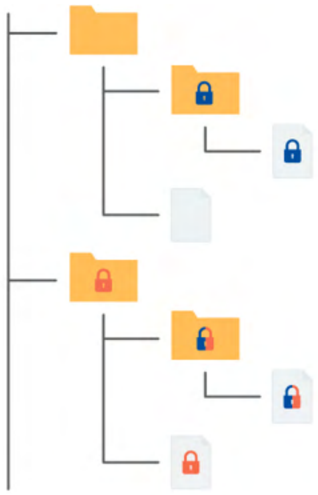


We decrypt and encrypt your files on demand: Do you want to view your content? Just tap on it and we download and decrypt your file for you. Are you finished with writing your essay? Just send it to Boxcryptor and we encrypt the file and store it into the cloud.

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 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.

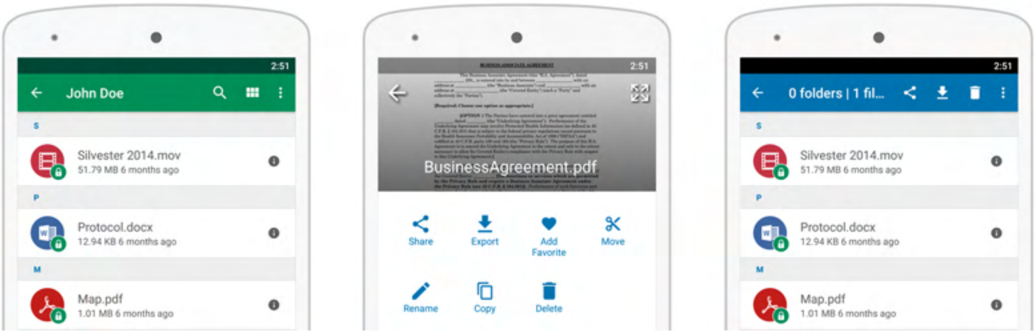
The Boxcryptor app is a general-purpose **file browser**. You can browse into folders or preview files by tapping on them. Boxcryptor will **automatically download and decrypt files** for you. You can upload files, create a new file, create a new folder, or take an encrypted photo by tapping on +.

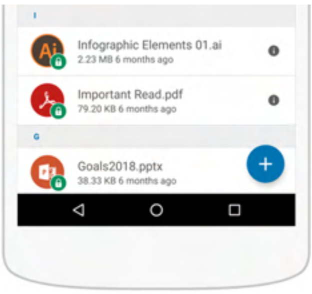
If you tap on a file longer, the file browser will switch to **Operation Mode**. In this mode, you can select files and folders by tapping on them. All available operations, such as **copy, move, rename or delete** can be triggered via the bar at the top.

Tapping on ⓘ opens the **File Details Bar**. In this bar you see a **preview of the file and you can trigger basic functions**, such as copy, move, rename or delete.

Besides that, Boxcryptor allows you to mark a file as a **favorite**. All files marked as **favorite** can be easily accessed via ☰ → **Favorites**.

The activities view (☰ → **Activities**) displays all files which have been changed recently.





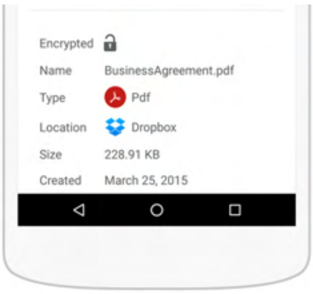
I

Infographic Elements 01.ai
2.23 MB 6 months ago

Important Read.pdf
79.20 KB 6 months ago

G

Goals2018.pptx
38.33 KB 6 months ago



Encrypted

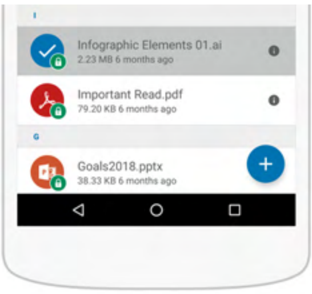
Name BusinessAgreement.pdf

Type Pdf

Location Dropbox

Size 228.91 KB

Created March 25, 2015



I

Infographic Elements 01.ai
2.23 MB 6 months ago

Important Read.pdf
79.20 KB 6 months ago

G

Goals2018.pptx
38.33 KB 6 months ago

Editing Files

Editing files on Android is a bit trickier than on other platforms. To increase security, Android sandboxes apps. This means that each app can only access its own folder on the system. Therefore, installed apps cannot access any data of other apps.

The problem is that if you send or share a file with another app, such as Word, the file is in fact copied to another place and Boxcryptor cannot access it anymore.

For this purpose we integrated Boxcryptor into Android's Storage Access Framework, which can be accessed by these other apps. If you want to edit files, make sure to always work directly within the third party app, not Boxcryptor. For instance, if you want to edit a Word file, open Word → select **Open other documents** on the **Open** tab, → **Browse** → ☰ → select **Boxcryptor**.

How to Recognize Encrypted Files

Boxcryptor allows you to have **encrypted and unencrypted** files and folders. Encrypted files or folders are marked with badge icons. Before creating new files or directories, you can decide whether these items should be encrypted or not.

🔒 **encrypted**

Encrypt Existing Files and Folders

Encrypting already existing files is currently not possible with Boxcryptor for Android. Please use Boxcryptor for Windows, Boxcryptor for macOS 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: 恂悰挦抱砻抮殡枏瞻攡敱漢快搬濂檬浉楻挭抧柜欅䀣.bc

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

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

Go to ☰ → **Settings** → **General** and switch on **Use 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 Windows, Boxcryptor for macOS or Boxcryptor Portable.
- If you want to copy or move your files to another location or app in decrypted mode, the file browser allows you to view an unecrypted version and export this version to other apps.

Camera Upload

The Camera Upload backs up any photo or video you take with your smartphone or tablet. 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.

To enable Camera Upload, follow these steps:

1. Tap on ☰ → Settings
2. Tap on **Enable Camera Upload**.
3. Select the cloud/location you want to upload to. If you have only one cloud/location added to Boxcryptor, it will be displayed and selected automatically.

4. Select if you only want to upload via Wi-Fi connection, or via mobile connection (data plan) as well.
5. To disable Camera Upload tap on **Enable Camera Upload** again.

How to Work With Offline Files

The **Offline Files** feature allows you to access your encrypted files at any time even without an internet connection.

To do this, you can select the desired file and make it available offline by clicking on ⋮ The encrypted file is then available under **Offline Files**.

When an Offline File is updated in the cloud, it updates automatically after about 15 minutes. However, it is also possible to start a manual synchronization:

Go to **Offline Files** in the main menu, tap on ⋮ and tap **Syncronize**.

If you make a change to an Offline File, an automatic upload will start as usual.

ⓘ The **Offline Files** feature is available to you from **version 2.85.736**.

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

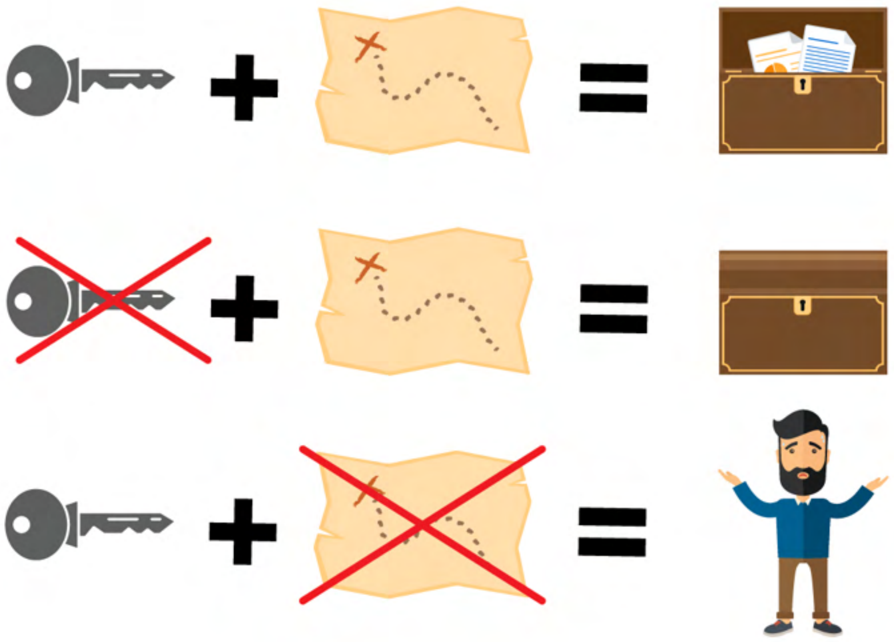
For understanding how the sharing of encrypted files works, it is helpful to understand how programs handle unencrypted and encrypted files.

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**.

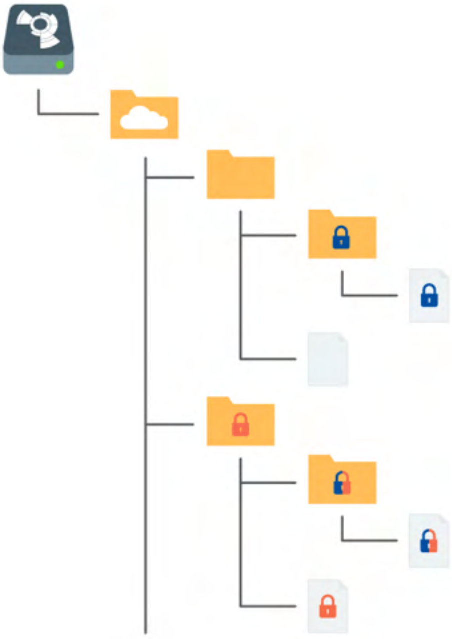
As a consequence, there are two steps necessary to share an encrypted file:

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 Android. Please use Boxcryptor for Windows or Boxcryptor for macOS 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 Android. 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

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

When this feature is enabled, you must authenticate with a method set in your device to use Boxcryptor.

To use the app protection, at least one of the following protection methods must be enabled in the **security settings of the device**:

- **Pattern**
- **PIN**
- **Password**
- **Fingerprint** (if hardware available)
- **Face Unlock** (if hardware available)

Depending on the hardware manufacturer, the available protection methods in Boxcryptor may vary. For some devices, a **preferred biometric authentication method** can be selected.

App protection is activated as soon as the app is in the background or the device is locked. If the user uses a **biometric** authentication method, he or she can also unlock Boxcryptor using an alternative method.

> Boxcryptor’s app protection uses the latest **AndroidX Biometric Library**. Compatibility issues may occur on some devices with a modified authentication screen. In the event of problems, we recommend that you avoid using alternative protection methods until the device manufacturer solved the problem.

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.
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:

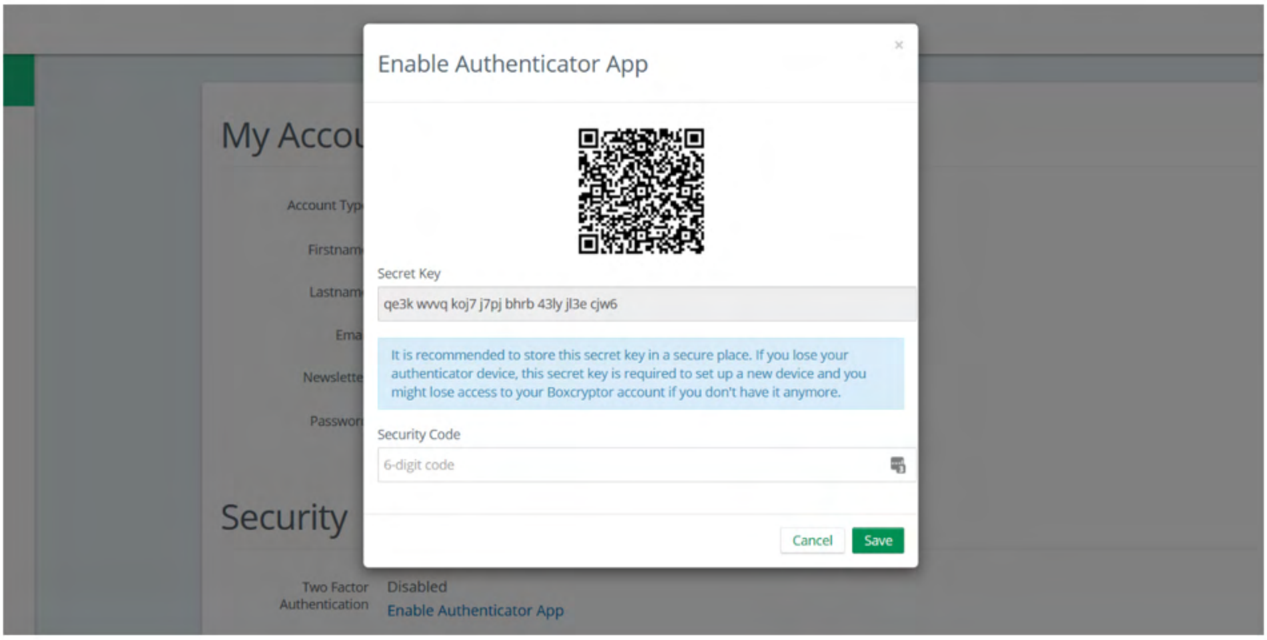
1. Sign in to boxcryptor.com.
2. Navigate to **Security**.
3. Click on **Two-factor Authentication -> Authenticator App**.
4. Scan the QR code with your Authenticator App. Copy the **Secret Key** and store it in a secure place.
5. To complete the setup, enter the 6-digit code from your authenticator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

Cancel Save

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.

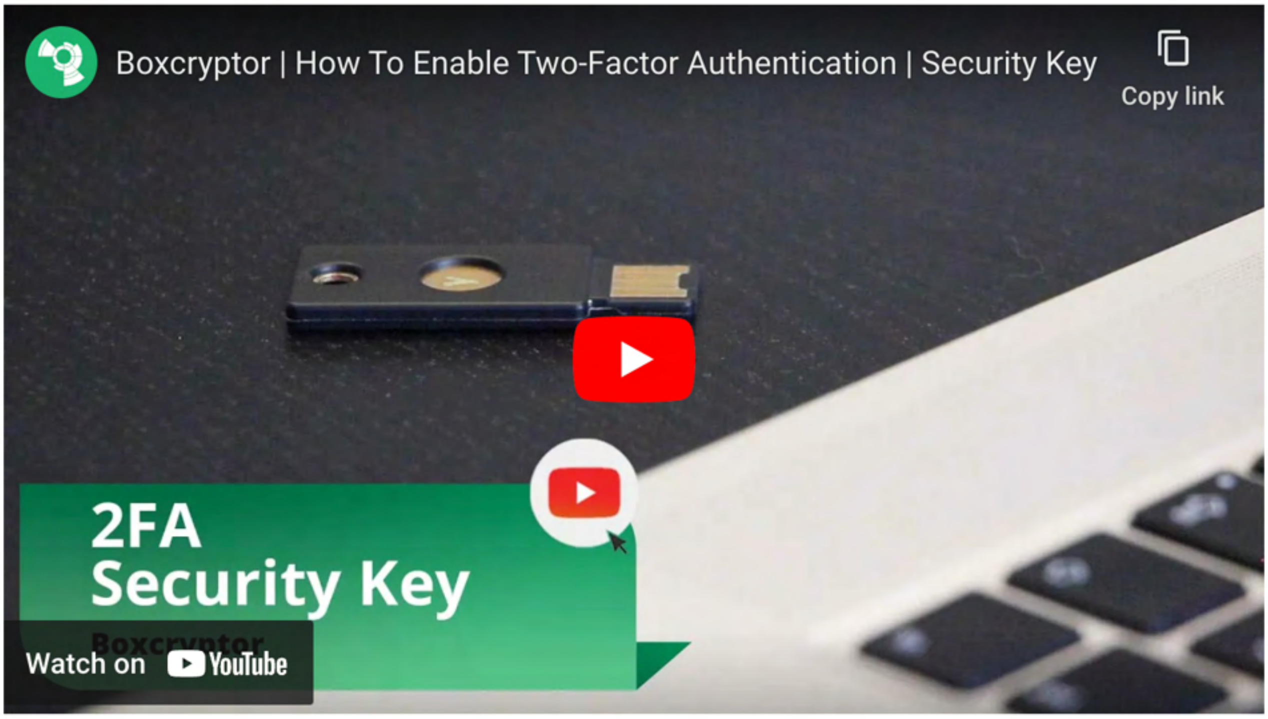
Security Keys

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

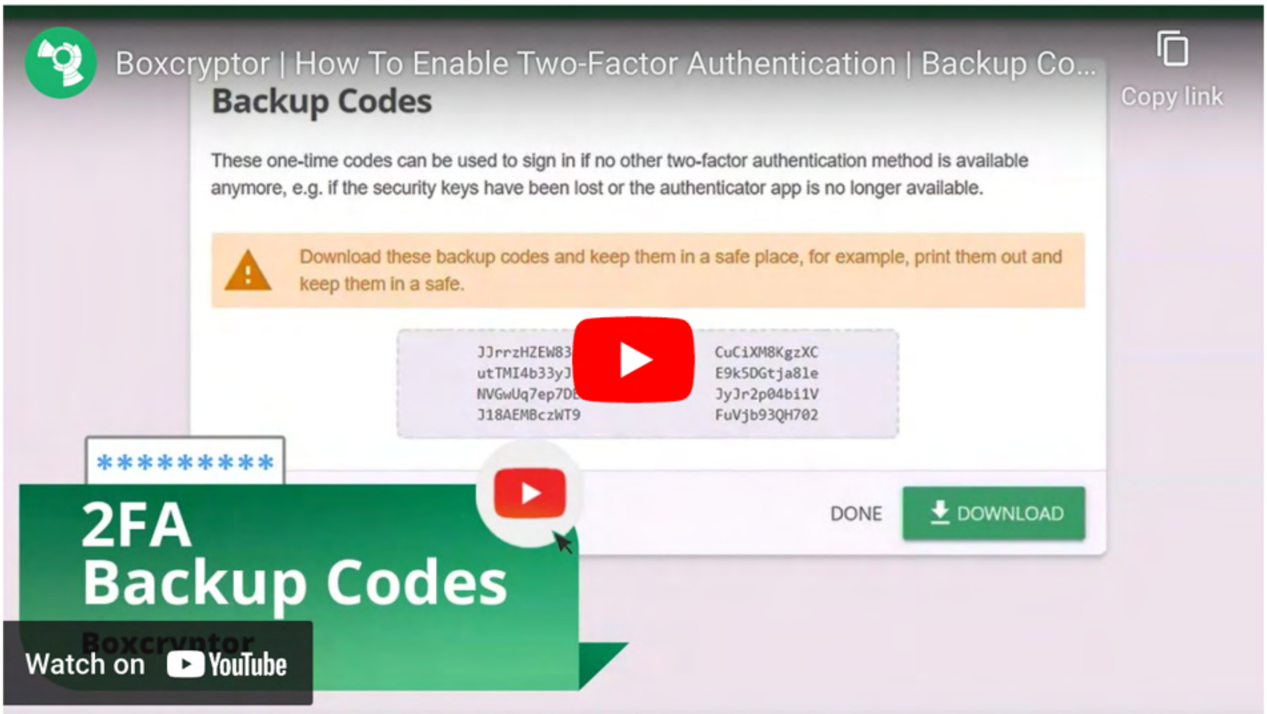
To prevent a lockout we recommend registering two security keys. Use one regularly, keep the other one as backup in case that you loose the first one. Alternatively, you can set up TOTP as a second factor backup.

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.



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 strongly recommend using our Desktop applications Boxcryptor for Windows or Boxcryptor for macOS.

If you cannot access your files on these platforms, please use the `Download` feature that is available on files in the Boxcryptor file Browser.

If you have whole folder structures you need to export, we recommend using a third-party tool that can access Boxcryptor via the "Storage Access Framework": Files

Here, you can browse the Boxcryptor Location and `long-press -> copy` any encrypted folder and paste it, e.g. into your `Download` folder.

Note: Make sure to disable Boxcryptor's "App Protection" to enable access via the Storage Access Framework.

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.

I Cannot Connect to the Boxcryptor Servers

Proxy Support

Boxcryptor uses the proxy configuration provided by the Android system.

Help can be found here at **Advanced Network Settings** → **Proxy**.

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 as a **user certificate** on your Android device. For more information, please see here.

> For self-signed certificates, the following configuration entry is required at creation to be accepted as a valid root CA:
> **`basicConstraints=CA:TRUE`**

> 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 no expect this much data usage for a simple move/copy operation, we decided to disable the option to move and copy between encrypted folders.

Camera Upload is Not Working

If Camera Upload is not working, please try the following:

- **Force quit**: Do not force quit Boxcryptor using an app manager or the Android app settings, as this will also force quit any background detection. Just **restart** Boxcryptor to enable background detection again.
- **Battery saver**: If the Android Battery Saver mode is enabled, any background detection is blocked. You can start Boxcryptor to bring it to the foreground so that the detection can run, or just disable the Android Battery Saver mode.
- **Battery optimization**: Android automatically battery optimizes any installed app. But this may cause issues if a process - like detecting photos or videos - must run in the background. You can **whitelist Boxcryptor** from battery optimization by heading to the **Android settings** → **battery** → ⋮ → **battery optimization** → **all apps**. Scroll to Boxcryptor, and select "Do not optimize".
- **Restart Boxcryptor**: In some cases it is sufficient to restart Boxcryptor. Swipe away Boxcryptor from the Android recent apps screen and start Boxcryptor again so that the Camera Upload detection is started.

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 Android is not available in Google Play anymore but can be downloaded it here: https://www.boxcryptor.com/download/Boxcryptor_Classic_v1.5.4_Android.apk *Supports Android 2.1, 3, 4*

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.

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

Gaps in the changelog represent internal test versions.

Version 2.122.1101 (2022-10-18)

- Fixed download issues on Dropbox
- Minor bugfixes and improvements

Version 2.121.1099 (2022-09-20)

- Fixed startup issues on Android 6

Version 2.120.1098 (2022-09-15)

- Fixed issues due to which uploads were not allowed to start
- Fixed issues where details for failed uploads were not available
- Fixed issues with video preview
- Reduced memory consumption
- Minor bugfixes and improvements

Version 2.119.1095 (2022-09-01)

> ⓘ This version has **official support for Android 13**.

- Official Android 13 support
- Fixed issues when sharing files with other apps
- Improved performance
- Minor bugfixes and improvements

Version 2.116.1072 (2022-08-03)

- Fixed issues with automatic camera upload
- Minor bugfixes and improvements

Version 2.115.1066 (2022-06-09)

- We added zoom functionality for the in-App Camera
- Favourites and offline files are now also displayed in the Storage Access Framework
- Fixed issues where files couldn't get uploaded to IONOS
- Minor bugfixes and improvements

Version 2.114.1057 (2022-04-06)

- Fixed issues while working without internet connection
- Fixed issues where uploads or downloads could get stuck in waiting state
- Fixed issues with special Google Drive file types
- Minor bugfixes and improvements

Version 2.113.1054 (2022-02-03)

- Fixed issues with uploading multiple files
- Fixed issues when working in external applications
- Fixed issues with Google Drive shortcuts
- Fixed issues where the specified network type was ignored for downloading files available offline
- Fixed issues with previewing audio and video files
- Minor bugfixes and improvements

Version 2.112.1047 (2021-12-06)

- Minor bug fixes and improvements

Version 2.111.1042 (2021-12-01)

- Support new MagentaCLOUD

Version 2.110.1036 (2021-10-19)

- Minor bug fixes and improvements

Version 2.109.1034 (2021-10-04)

This version has **official support for Android 12**.

This version **does not support Android Lollipop (5)** anymore. As this old version is not supported by Google anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- Official Android 12 support
- Minor bug fixes and improvements

Version 2.108.1021 (2021-08-04)

- We added Microsoft Teams to our supported cloud storage provider list
- We added dark mode support
- Changed colour scheme of the user interface
- Fixed caching issues

Version 2.107.1005 (2021-06-23)

- When using the automatic camera upload, thumbnails are now regularly generated, regardless of the device with which the photos were taken.
- Fixed issues with adding 2FA secured cloud storage provider
- Bug fixes and improvements

Version 2.106.992 (2021-05-10)

- Fixed issues when uploading files from external apps
- Fixed camera upload issues
- Fixed offline file issues
- Fixed issues when working with big files
- Fixed issues with thumbnail generation
- Improved performance when working with bad internet connection
- Minor bug fixes and improvements

Version 2.105.935 (2020-12-04)

- Fixed issues with adding 2FA secured cloud storage provider on pixel devices.
- Fixed issues with accessing Whisply shared files.
- Fixed issues with accessing mail.ru Hotbox.
- Minor bug fixes and improvements

Version 2.104.916 (2020-11-10)

- Files can now be downloaded to the device.
- Fixed issues with adding a cloud storage provider.
- Fixed issues with saving files from other apps.
- Fixed issues with local key files.

- Minor bug fixes and improvements

Version 2.103.895 (2020-09-29)

- Google Drive shortcuts support
- Minor bug fixes and improvements

Version 2.102.884 (2020-09-01)

- Official Android 11 support
- Improved WebDAV performance
- Minor bug fixes and improvements

Version 2.101.875 (2020-08-07)

- Fixed issues with camera upload permissions on Android 10

Version 2.100.873 (2020-08-05)

- Fixed issues with Dropbox Vault
- Fixed performance issues with Strato HiDrive and Telekom MagentaCLOUD
- Improved stability
- Minor Bugfixes and improvements

Version 2.99.838 (2020-04-18)

- Fix OneDrive Germany Authentication
- Fix storage authentication after failure
- Improved Google Drive performance
- Improved Upload stability
- Reduce memory usage for thumbnail generation
- Minor bugfixes and improvements

Version 2.98.822 (2020-04-07)

- We added LeitzCloud to our supported cloud storage provider list
- Bug fixes and improvements

Version 2.97.815 (2020-03-19)

- Bug fixes and improvements

Version 2.96.808 (2020-03-12)

- Bug fixes and improvements

Version 2.95.804 (2020-03-04)

- Improved filebrowser usability
- Bug fixes and improvements

Version 2.94.790 (2020-01-21)

- Bug fixes and improvements

Version 2.93.786 (2020-01-14)

- Bug fixes and improvements

Version 2.92.783 (2020-01-09)

- App Protection with system authentication methods
- Open office files directly from the browser
- Fixed web based storage provider authentication
- Bug fixes and improvements

Version 2.91.776 (2019-12-12)

- Bug fixes and improvements

Version 2.90.771 (2019-12-03)

- Adds IONOS HiDrive support
- Discontinued Orange Cloud support
- Improved overall performance
- Bug fixes and improvements

Version 2.89.747 (2019-10-23)

- Minor bug fixes and improvements

Version 2.88.746 (2019-10-07)

- Minor bug fixes and improvements

Version 2.87.745 (2019-09-26)

- Minor bug fixes and improvements

Version 2.86.740 (2019-09-04)

- Adds official Android 10 support
- Minor bug fixes and improvements

Version 2.85.736 (2019-08-27)

- Adds Offline Files. Make files offline available so they stay always on your device.
- Adds faster image preview if a thumbnail is already available.
- Minor bug fixes and improvements

Version 2.84.720 (2019-07-11)

- Adds thumbnails for downloaded and uploaded images
- Adds a grid view to the browser
- Adds new and beautiful file icons

- Better handling for conflicting files after editing
- Fixes issues with the Microsoft Office integration
- Minor bug fixes and improvements

Version 2.83.713 (2019-06-04)

We added Wasabi to our supported cloud storage provider list

Version 2.82.711 (2019-05-22)

- Minor bug fixes and improvements

Version 2.81.710 (2019-05-02)

- Minor bug fixes and improvements

Version 2.80.709 (2019-04-11)

- Minor bug fixes and improvements

Version 2.79.708 (2019-04-10)

- Minor bug fixes and improvements

Version 2.78.706 (2019-04-09)

We have completely reworked Boxcryptor with the following highlights:

- Faster download
- Faster upload
- Overall improved speed
- Modern user interface
- Overall improved user experience
- Improved camera upload
- Overall improved reliability

Version 2.77.687 (2018-09-06)

- Minor bug fixes and improvements

Version 2.76.673 (2018-08-03)

- Minor bug fixes and improvements

Version 2.75.662 (2018-07-20)

- Minor bug fixes and improvements

Version 2.74.661 (2018-07-12)

- Improved: Sorting of filenames containing numbers
- Improved: Detection of several file types to open files in correct app
- Fixed: Several issues during upload

- Fixed: Show notifications on Android 8
- Minor bug fixes and improvements

Version 2.73.634 (2018-05-11)

- Added: Dropbox Team Space support
- Added: Enter Sharepoint Site URL
- Minor bug fixes and improvements

Version 2.72.627 (2018-02-26)

- Added: ownCloud support
- Added: Nextcloud support
- Minor bug fixes and improvements

Version 2.71.614 (2017-12-18)

- Minor bug fixes and improvements

Version 2.70.613 (2017-12-13)

- Improved: Faster Startup
- Minor bug fixes and improvements

Version 2.69.609 (2017-11-07)

- Improved: Storage Provider Communication
- Improved: Orange Authentication
- Minor bug fixes and improvements

Version 2.68.606 (2017-09-18)

- Fixed: WebDAV credentials input

Version 2.67.605 (2017-09-18)

- Fixed: Telekom Secure Data Drive
- Minor bug fixes and improvements

Version 2.66.604 (2017-09-07)

- New: Major redesign of the user interface for creating accounts and signing in
- New: Nutstore support
- Improved: Storage provider error messages
- Minor bug fixes and improvements

Version 2.65.594 (2017-07-31)

- New: Fingerprint App Protection support
- Minor bug fixes and improvements

Version 2.64.591 (2017-07-17)

- New: Google Team Drives support
- Minor bug fixes and improvements

Version 2.63.590 (2017-07-04)

- Fixed: Local Storage Listing

Version 2.62.589 (2017-06-30)

- Minor bug fixes and improvements

Version 2.61.588 (2017-06-22)

- Improved: Camera Upload
- Minor bug fixes and improvements

Version 2.60.580 (2017-06-13)

- New: OneDrive for Business Germany support
- Fixed: Google Drive authentication
- Minor bug fixes and improvements

Version 2.59.575 (2017-04-12)

- Minor bug fixes and improvements

Version 2.58.574 (2017-04-11)

- New: Chromebook Support
- New: Chrome Tab support for Strato HiDrive
- Fixed: Chrome Tab not working on some devices
- Fixed: OneDrive upload
- Fixed: CloudMe sign in
- Fixed: Egnyte listing
- Minor bug fixes and improvements

Version 2.56.569 (2017-03-28)

- New: mail.ru Hotbox support
- New: Cancel operations in browser view
- Improved: App Unlock experience
- Improved: Network stability
- Fixed: Microsoft Office files open read-only
- Minor bug fixes and improvements

Version 2.55.568 (2017-02-27)

- New: Take a Photo directly in Boxcryptor
- New: PDF Preview
- New: Download Progress in Previewer
- New: Chrome Tab support for Provider Credentials
- Improved: Russian Texts

- Improved: Speed & Stability
- Minor bug fixes and improvements

Version 2.54.565 (2017-01-17)

- Improved: Orange Cloud support. Please re-add your account
- Fixed: Box & hubiC download
- Minor bug fixes and improvements

Version 2.53.563 (2016-12-21)

- Minor bug fixes and improvements

Version 2.52.562 (2016-12-09)

- Fixed: Files sent to Boxcryptor lost their filename when uploading

Version 2.51.561 (2016-11-25)

- Minor bug fixes and improvements

Version 2.50.560 (2016-11-25)

- Minor bug fixes and improvements

Version 2.49.559 (2016-11-17)

- Improved: Browsing experience
- Fixed: Amazon Cloud Drive issues
- Minor bug fixes and improvements

Version 2.48.557 (2016-11-03)

- New: SharePoint Online suppor
- New: Show Recent Activities
- Improved: Yandex support. Please re-add your accoun
- Improved: SD-card suppor
- Improved: PIN code handlin
- Major internal code improvement
- Minor bug fixes and improvements

Version 2.1.447.546 (2016-08-25)

- Improved: Network stability
- Fixed: mailbox.org Drive WebDAV url
- Minor bug fixes and improvements

Version 2.1.446.544 (2016-08-18)

- Improved: Dropbox support
- Fixed: OneDrive (for Business) listing of folders with many entries
- Minor bug fixes and improvements

Version 2.1.445.539 (2016-08-04)

- Fixed: When using local storage, the parent directory could get deleted on file upload

Version 2.1.444.537 (2016-07-27)

- New: Favorites
- New: Boxcryptor color
- New: "Show password" button
- Improved: Faster and more stable sign in
- Improved: Telekom MagentaCLOUD support. Please re-add your account
- Fixed: Filename and permission inheritance
- Fixed: OneDrive (for Business) shared folders access
- Minor bug fixes and improvements

Version 2.1.417.536 (2016-05-13)

- New: hubiC support
- New: Create Microsoft Office files
- Improved: Strato HiDrive support. Please re-add your account
- Removed: Barracuda Copy support
- Fixed: OneDrive (for Business) issues
- Minor bug fixes and improvements

Version 2.1.417.535 (2016-04-20)

- Fixed: OneDrive (for Business) issues
- Minor bug fixes and improvements

Version 2.1.417.533 (2016-04-06)

- Added: Set Remember Password in Settings
- Added: Change Password in Settings
- Fixed: Possible OneDrive (for Business) folder listing issues
- Minor bug fixes and improvements

Version 2.1.417.532 (2016-03-30)

- New: Full Storage Access Framework support. Save and open encrypted files from other apps
- Improved: OneDrive (for Business) support. Please re-add your OneDrive (for Business) account
- Removed: Filespots support
- Minor bug fixes and improvements

Version 2.1.417.531 (2016-02-25)

- Fixed: Telekom Mediencenter is now MagentaCLOUD
- Minor bug fixes and improvements

Version 2.1.417.530 (2016-01-25)

- Minor bug fixes and improvements

Version 2.1.417.529 (2016-01-18)

- Minor bug fixes and improvements

Version 2.1.417.528 (2015-12-23)

- Minor bug fixes and improvements

Version 2.1.417.527 (2015-12-21)

- New: Android Access Storage Framework Support
- New: Rename cloud storage providers
- Improved: SD card support
- Minor bug fixes and improvements

Version 2.1.417.520 (2015-10-21)

- Fixed: Android 6.0 Permissions
- Fixed: Box Authorization
- Minor bug fixes and improvements

Version 2.1.417.519 (2015-09-30)

- Improved: File preview
- Improved: Settings screen
- Improved: Sorting of files and folders
- Added: Fastscroll in browser
- Minor bug fixes and improvements

Version 2.1.417.517 (2015-08-18)

- Minor bug fixes and improvements

Version 2.1.417.514 (2015-06-28)

- New: Material Design User Interface
- Added: Copy.com support
- Added: Orange Cloud support
- Minor bug fixes and improvements

Version 2.1.417.510 (2015-06-17)

- Added: Automatic system proxy detection
- Added: Dropbox login using Dropbox app
- Fixed: Local Account issues
- Minor bug fixes and improvements

Version 2.1.417.508 (2014-05-20)

- Added: Amazon S3 support
- Improved: WebDAV self signed certificate support
- Improved: Login speed
- Fixed: Login screen was shown if camera upload was active

- Minor bug fixes and improvements

Version 2.1.417.506 (2015-04-29)

- Added: Amazon Cloud Drive support

Version 2.1.415.498 (2014-12-15)

- Minor bug fixes and improvements

Version 2.1.415.496 (2014-12-11)

- Minor bug fixes and improvements

Version 2.1.415.493 (2014-11-26)

- Fixed: Box upload not working
- Fixed: Rename removes .bc ending
- Minor bug fixes and improvements

Version 2.1.413.484 (2014-07-29)

- Minor bug fixes and improvements

Version 2.1.413.483 (2014-07-14)

- Fixed: Account created on Android not working on other platforms
- Fixed: Switching between Local/Boxcryptor Account
- Minor bug fixes and improvements

Version 2.1.413.479 (2014-07-08)

- Added: Automatic camera upload (requires new permission: Run at startup)
- Added: Search provider- and browserlist
- Added: Create text file
- Added: PSMail Cabinet support
- Improved: Browser Performance
- Fixed: Provider 2-Factor-Authentication not working
- Minor bug fixes and improvements

Version 2.0.411.27 (2014-04-09)

- Added: Login, browse folders and open files you have already visited without internet connection
- Added: Photo thumbnails when uploading photos
- Added: OneDrive for Business support
- Added: Storegate support
- Added: mailbox.org support
- Fixed: Some files could not be decrypted
- Minor bug fixes and improvements

Version 2.0.409.25 (2014-02-25)

- Fixed: New encrypted folder could not be read on other platforms
- Modified: Renamed SkyDrive to OneDrive
- Minor bug fixes and improvements

Version 2.0.409.24 (2014-02-20)

- Added: Sort by creation date
- Added: Google Drive support to Kindle devices
- Improved: Adding cloud provider
- Fixed: Dropbox could not be added
- Fixed: Text Editor set wrong newlines
- Removed: No longer needed permissions
- Minor bug fixes and improvements

Version 2.0.407.23 (2013-12-16)

- Fixed: Cloud providers are not stored
- Modified: Updated Box
- Minor bug fixes and improvements

Version 2.0.405.21 (2013-11-04)

- Fixed: Local account & local storage usage without Internet connection
- Minor bug fixes and improvements

Version 2.0.403.19 (2013-10-21)

- Some bug fixes

Version 2.0.403.18 (10/15/2013

- Added: Translations for German, French, Spanish, Italian and Russian
- Added: PIN unlock
- Added: Support for CloudMe
- Added: Support for Grau DataSpace
- Fixed: Google Drive limits file listing
- Minor bug fixes and improvements

Version 2.0.402.17 (2013-09-24)

- Added: Image Preview Zoom
- Improved: File Preview
- Improved: User Interface
- Fixed: WebDAV issues
- Fixed: Logout on user changes
- Fixed: PRNG crash on some devices (e.g. Samsung Galaxy S4)
- Fixed: Smaller bugs

Version 2.0.402.16 (2013-08-21)

- Improved: Login Speed up to 5x faster
- Improved: User Interface

- Fixed: Android PRNG
- Fixed: FileSpots 401 Error
- Fixed: Dialog button order on older devices
- Fixed: Smaller issues

Version 2.0.402.14 (2013-07-23)

- Added: Boxcryptor Tour
- Added: Send files to Boxcryptor
- Added: Manage Uploads
- Added: Support for Filespots
- Improved: Performance
- Improved: Design
- Improved: Help/About Section
- Fixed: Login error messages
- Fixed: Smaller bugs

Version 2.0.401.13 (2013-06-25)

- Added: Support for local accounts using key files instead of the Boxcryptor Key Server
- Added: Warning if inside Boxcryptor Classic Folder
- Fixed: Small bugs

Version 2.0.400.10 (2013-06-12)

- Fixed: Could not get device id error due to missing entry of manufacturer
- Fixed: Crash when starting settings on xlarge tablets
- Fixed: Small reported bugs

Version 2.0.400.9 (2013-06-07)

- Fixed: Wrong credentials error due to wrong password hash calculation
- Fixed: Small reported bugs

Version 2.0.400.8 (2013-06-05)

- Initial Release

Network Access

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

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

```
Domain: api.boxcryptor.com
```

```
Port: 443
Protocol: HTTPS
IP Addresses: 136.243.125.202, 148.251.224.99, 188.40.161.201
```

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

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

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

Open Source Licenses

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

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