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 Windows 10 or later, .NET Framework >= 4.7.2 and WebView2 Runtime (If you run regular Windows Updates, it is very likely that .NET Framework and WebView2 Runtime is already installed).

⚠ Currently, Boxcryptor does not run natively on **ARM**-based Windows 10 / 11 devices. However, we are working to support the ARM architecture in the near future.

ℹ Boxcryptor is officially not supported on **Windows Insider Previews**. Those experimental Windows versions can make apps unusable without any previous warnings. If you experience difficulties, you will find help at *Go back to your previous version of Windows*.

To install Boxcryptor on your Windows computer, follow these 3 steps:

1. Install the desktop application of your cloud provider.
2. Download Boxcryptor for Windows.
3. Run the installer and follow the instructions in the Wizard.

You will be asked to allow the installation of device software published by Callback Technologies (formerly EldoS Corporation). This is a **required** component of Boxcryptor. Therefore, when you are asked to install the software, please click **Install**. The installation temporarily closes some applications including your desktop. After installation, these applications will be restarted automatically.

Create a Boxcryptor Account

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

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

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

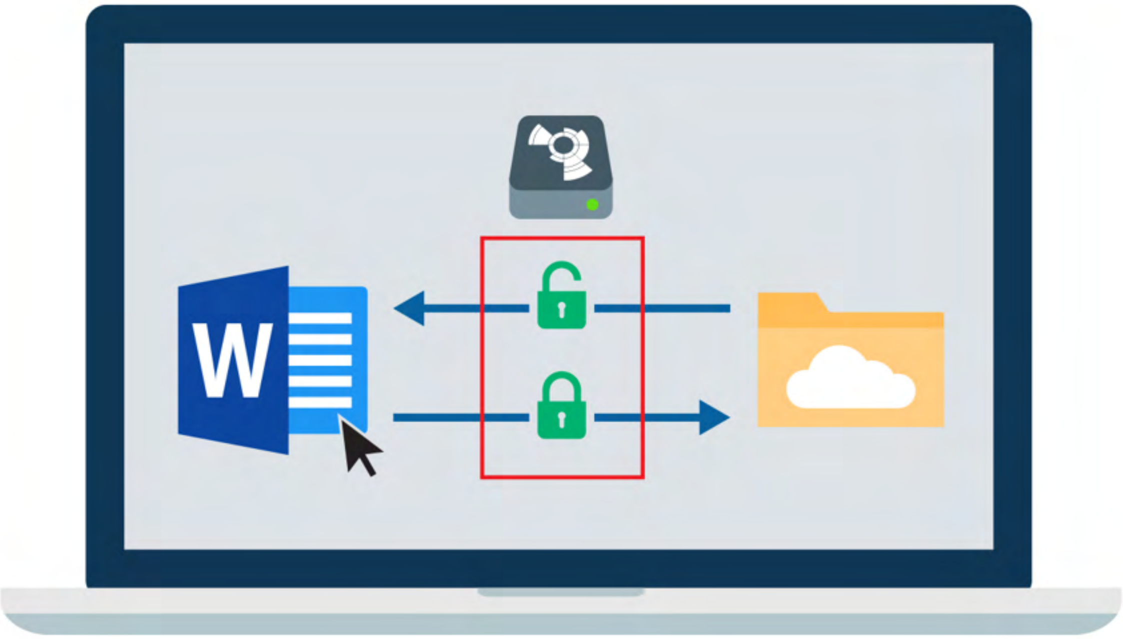
Create a password that you can remember, or store the password in a secure place, for example a password manager. Boxcryptor is a zero knowledge encryption software, therefore we **cannot** restore your password.

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

Discover Boxcryptor

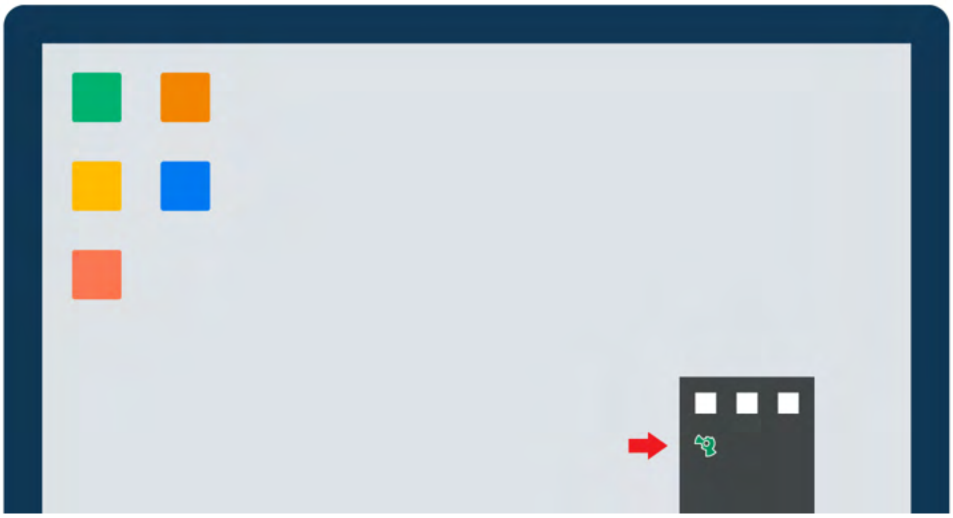
Once you have installed Boxcryptor and signed in to your account, you can access the **Boxcryptor drive** with the drive letter **X:**.

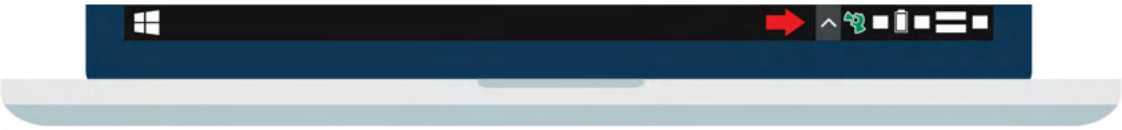
Boxcryptor will automatically add all installed cloud providers to the drive. From now on you can find all your clouds here. The drive acts like a layer on top of your existing files. It enables you to view, edit, and save your encrypted files on-the-fly.



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

Note: You can open your Boxcryptor Drive by double clicking on the Boxcryptor logo in your system tray right next to the clock.





Your First Encrypted Folder

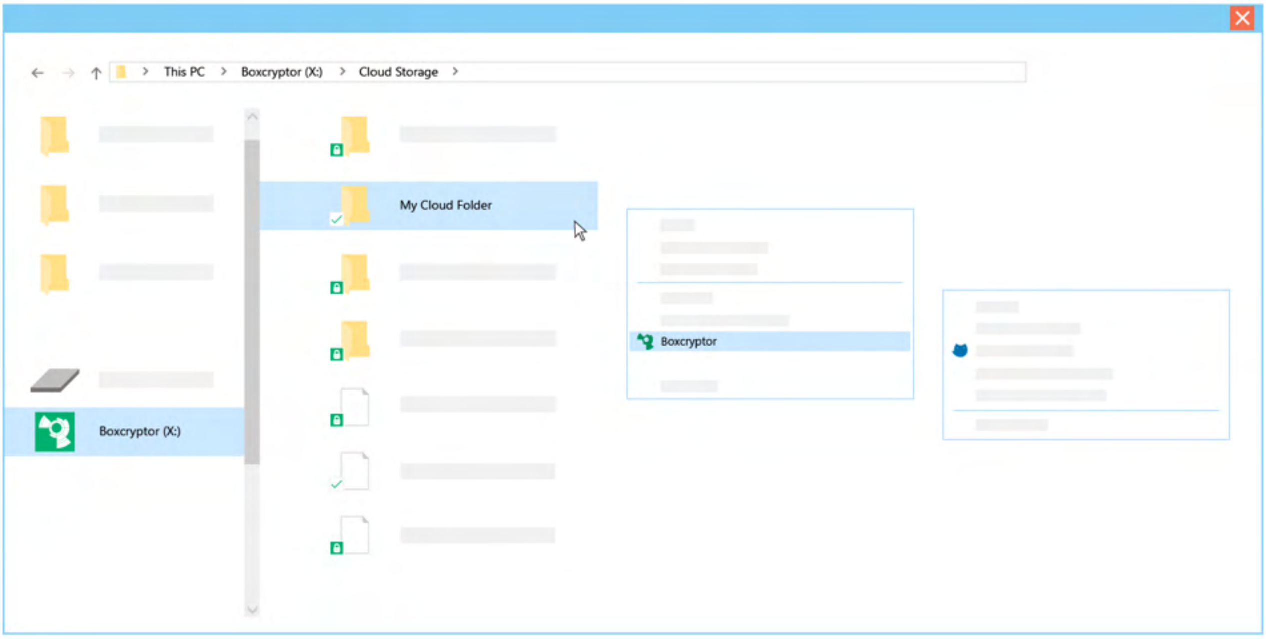
All files and folders that you add to an **encrypted folder** in Boxcryptor will be **encrypted automatically**. If you are new to Boxcryptor and do not have any files in your cloud yet, this is how you get started.

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

How to Encrypt Existing Files

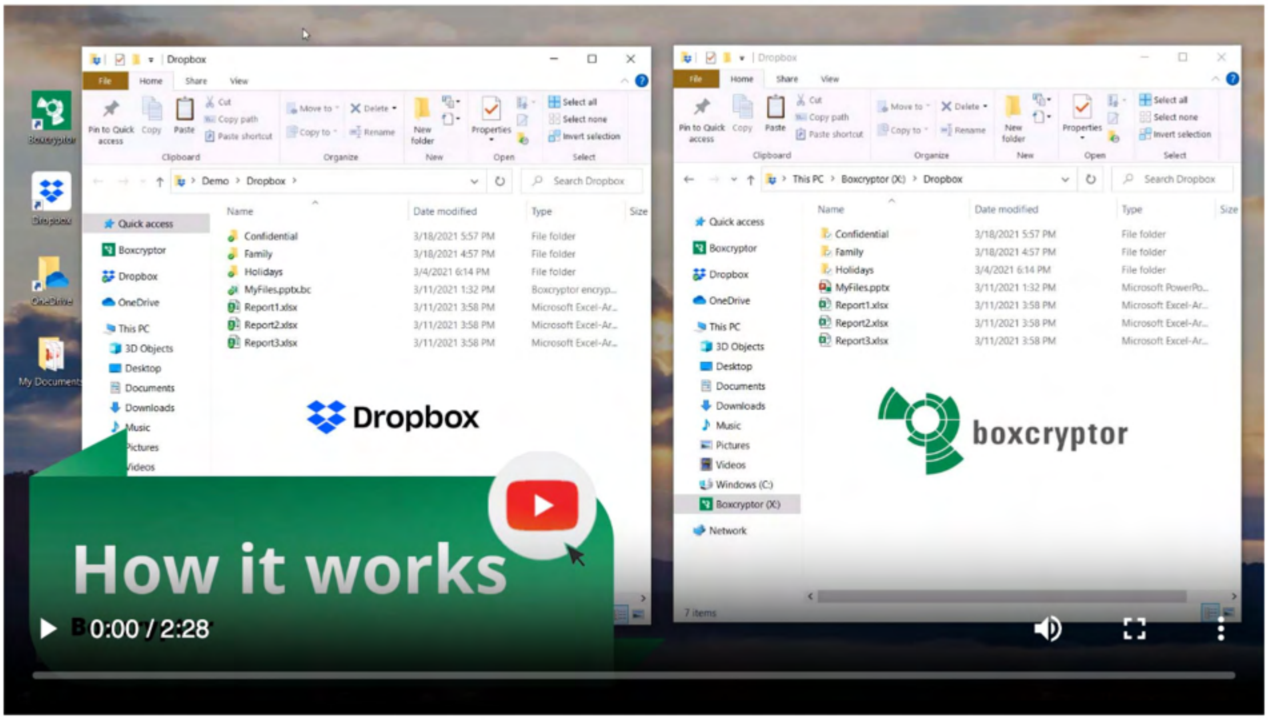
If you already have files and folders in your cloud, Boxcryptor can encrypt these existing files as well.

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



Note: The overlay icons in the Boxcryptor drive will tell you when synchronization and encryption are done. However, this only works when your cloud provider supports this feature.

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



Demo > Dropbox

Name	Date modified	Type	Size
Confidential	3/18/2021 5:57 PM	File folder	
Family	3/18/2021 4:57 PM	File folder	
Holidays	3/4/2021 6:14 PM	File folder	
MyFiles.pptx.bc	3/11/2021 1:32 PM	Boxcryptor encryp...	
Report1.xlsx	3/11/2021 3:58 PM	Microsoft Excel-Ar...	
Report2.xlsx	3/11/2021 3:58 PM	Microsoft Excel-Ar...	
Report3.xlsx	3/11/2021 3:58 PM	Microsoft Excel-Ar...	

This PC > Boxcryptor (X:) > Dropbox

Name	Date modified	Type	Size
Confidential	3/18/2021 5:57 PM	File folder	
Family	3/18/2021 4:57 PM	File folder	
Holidays	3/4/2021 6:14 PM	File folder	
MyFiles.pptx	3/11/2021 1:32 PM	Microsoft PowerPo...	
Report1.xlsx	3/11/2021 3:58 PM	Microsoft Excel-Ar...	
Report2.xlsx	3/11/2021 3:58 PM	Microsoft Excel-Ar...	
Report3.xlsx	3/11/2021 3:58 PM	Microsoft Excel-Ar...	

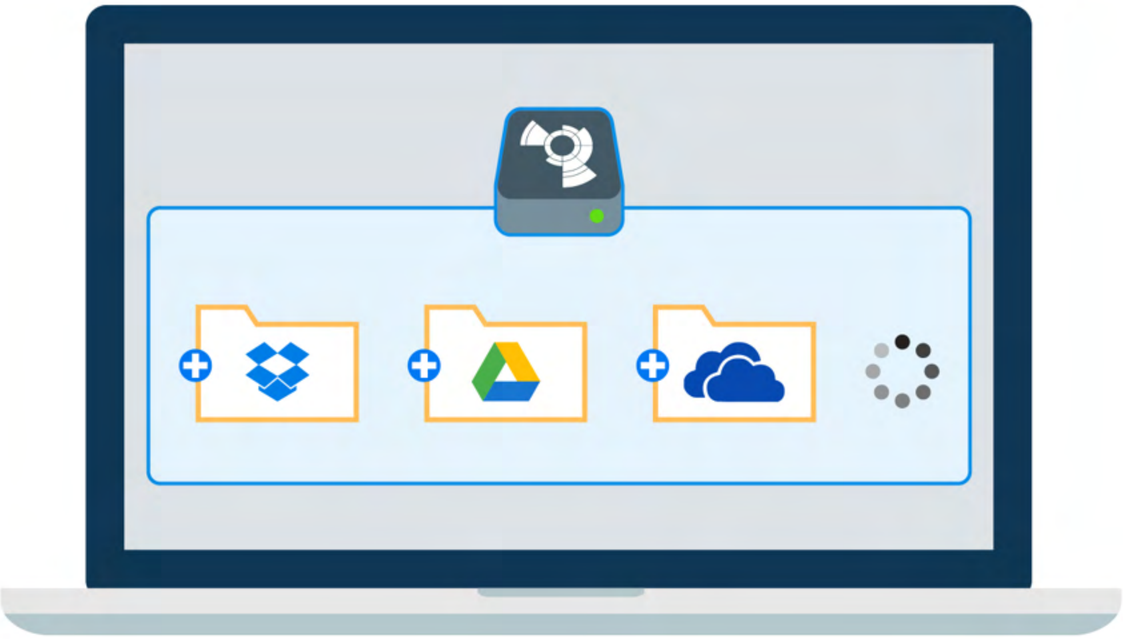
Manage Clouds and Locations

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

Cloud Storages

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

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



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

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

Google Drive

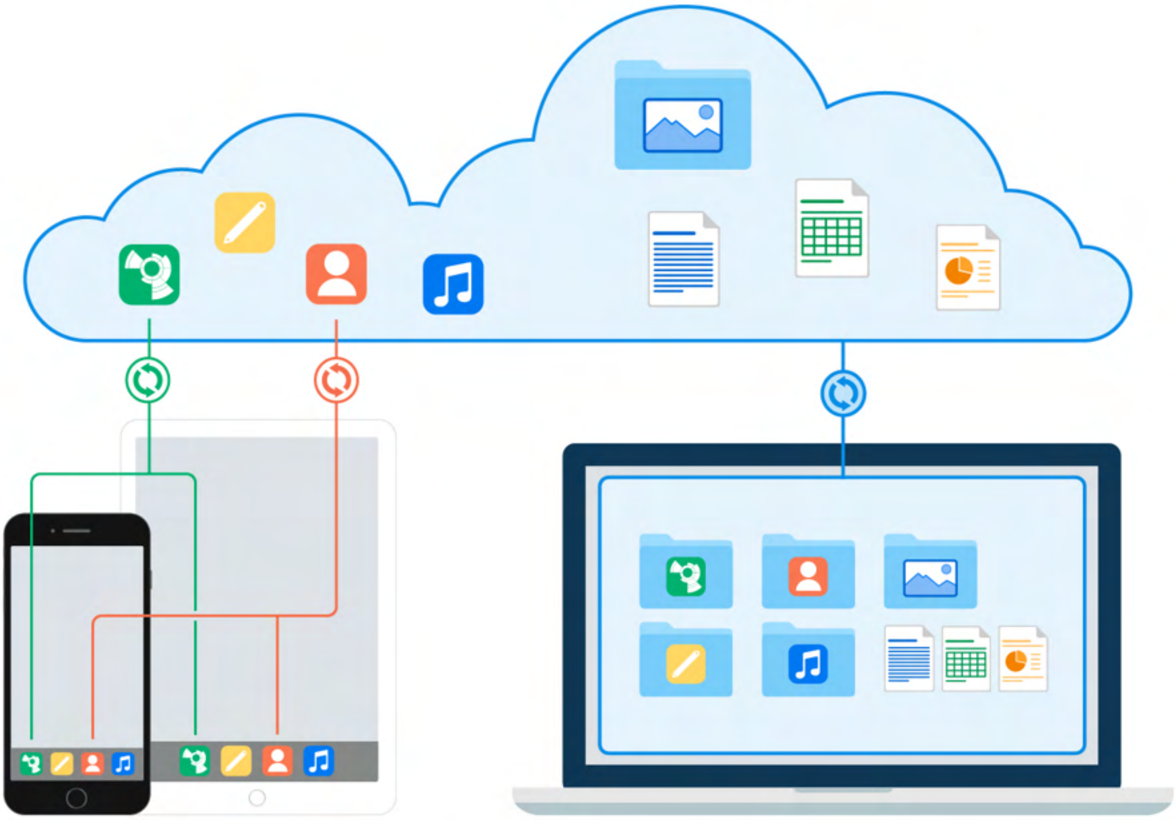
Boxcryptor automatically detects both your Google Drive **mirrored** and **streamed** locations. **Any additional backed up folder is not added automatically.**

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

Shared drives are currently only supported in **streamed** locations.

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 PC.

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

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

1. Install Boxcryptor on your iPhone or iPad and also on your desktop devices.
2. Make sure that you are signed in to iCloud on all devices.
3. Add the **iCloud** provider in Boxcryptor for iOS.
4. Upload an encrypted file to **iCloud** via Boxcryptor for iOS.
5. Apple will then create a Boxcryptor folder in their cloud.
6. Open Boxcryptor on your desktop and access the **iCloud** location on macOS or **iCloud Drive** → **Boxcryptor** on Windows. You will find the encrypted file from your iPhone or iPad there.

7. To make files from your Mac or PC available on your iPhone or iPad, move or copy the files to the folders mentioned above. You will then have them available on your mobile and desktop devices.

Network Drives and USB Devices

Network drives and removable USB drives are detected automatically by Boxcryptor, too. As network drives may not always be available when Boxcryptor is running, they are not automatically removed. In order to remove old network drive locations, the auto-detection must temporarily be disabled.

> How to disable network or removable drive auto-detection

Custom Locations

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

Right-click the **Boxcryptor tray icon** → **Settings** → **Locations** → **Add** and then choose your very own location.

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

WebDAV Locations

You can add any cloud provider to Boxcryptor if it supports WebDAV, or SMB locations:

- Right-click the **Boxcryptor tray icon** → **Settings** → **Locations** → **Add**.
- Type in the correct **URL** in the folder's **address bar**.

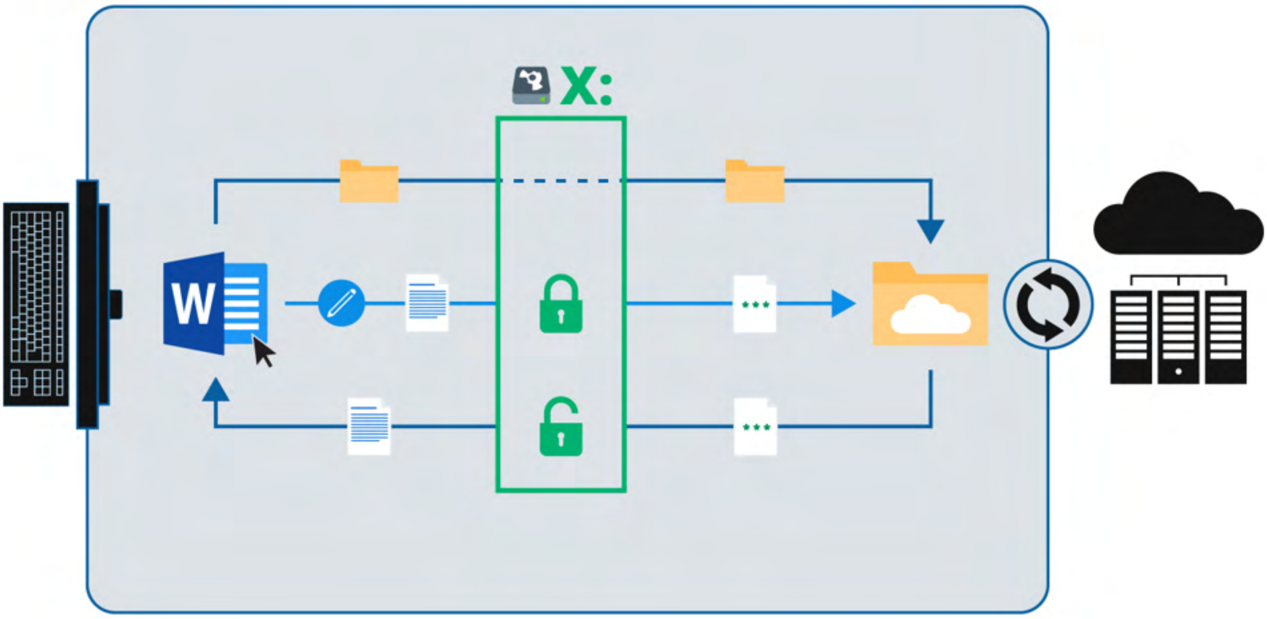
> ℹ Depending on the latency and bandwidth of your network or internet connection, directly adding network locations can have a severe negative impact on the overall Boxcryptor performance. Therefore, always favor a locally available folder instead of a network location.

Work With Files

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

On-the-fly Encryption

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

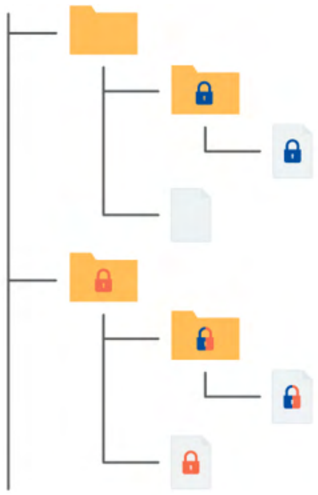


We accomplish this simplicity by creating a virtual drive on your machine. It acts like an **encryption-empowered window to your data**. All your files – whether they are encrypted or not – can be **accessed via this virtual Boxcryptor drive**.

Encryption and Permission Hierarchy

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

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



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

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

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

Note: If you add a file to a folder that is not encrypted, Boxcryptor will ask you if you want to encrypt it or not.

Work With Your Files

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

Boxcryptor deeply integrates into Windows by creating a virtual drive. The encryption takes place on-the-fly. Therefore, all other programs, including the Windows Explorer, will work the **same way as with files on your hard drive**.

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

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

How to Recognize Encrypted Files

Boxcryptor allows you to have **encrypted and unencrypted** files and folders. Encrypted files and folders in the Boxcryptor drive are **marked with small icons** that indicate their current state.

🔒 **encrypted** and **synchronized**

🔄 **encrypted** and synchronization **in progress**

> Dropbox Smart Sync online-only files will appear slightly greyed-out in the Boxcryptor

drive. See On-Demand Files for more info.

Encrypt Existing Files and Folders

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

- Browse to the file or folder you want to encrypt.
- Right-click the selection and chose **Boxcryptor** → **Encrypt** in the context menu.
- Wait for your cloud provider's sync client to sync everything.

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

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

Work With Filename Encryption

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

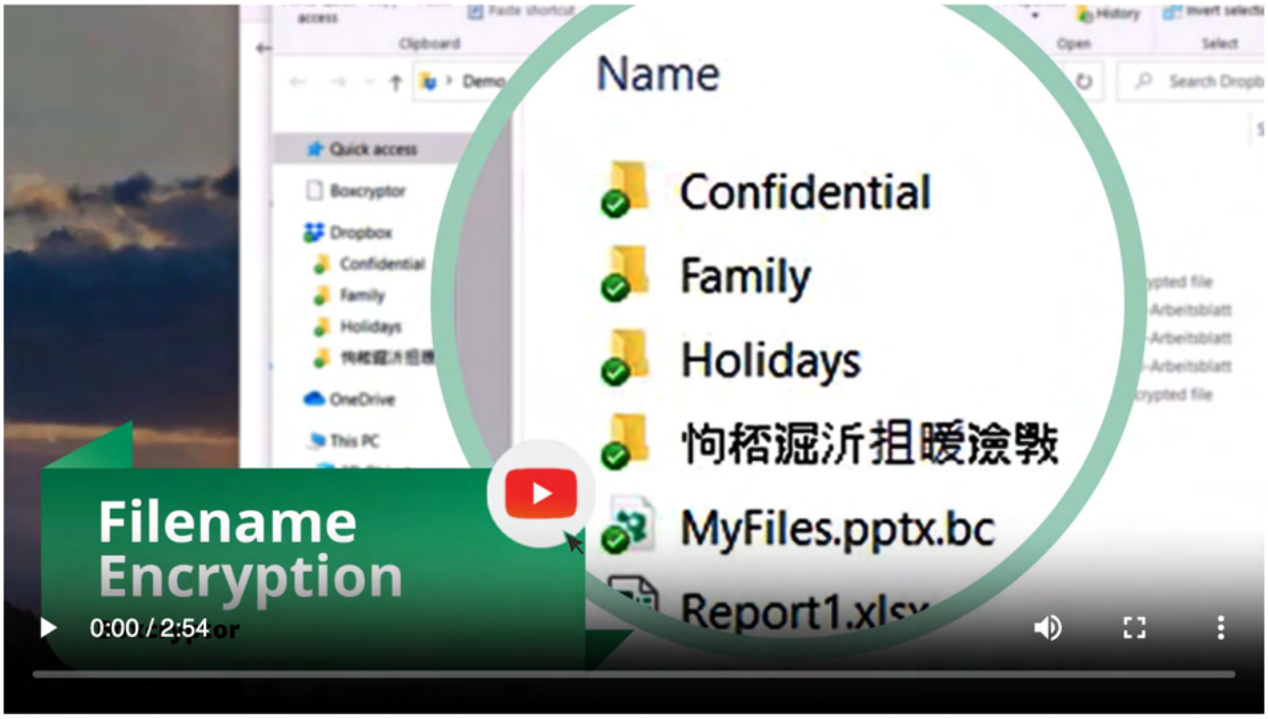
A filename encrypted file will look like this: 恂悰挦抱砦抮殨栮瞻擟敯漢快搬濂檬浉楻挭抧柜欅毖.bc

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

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

To activate filename encryption globally, go to **Boxcryptor Settings** → **Security** → **Encryption** and check **Enable filename encryption**.

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



How to Decrypt Files

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

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

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

On-Demand Files

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

Dropbox Smart Sync

Dropbox Smart Sync defines three states for files and folders:

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

- **Local content** is downloaded and saved on the hard drive of your computer. You can directly edit these files from applications on your computer.

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

The Smart Sync state of files is indicated by the file icon. The file icons of online-only files are faded or "grayed / whited" out.

Note: The Dropbox Smart Sync state of folders is not shown in the Boxcryptor drive. If you want to determine the Smart Sync state of a folder, right-click it and choose **Boxcryptor → Show Original in Dropbox**. You can then identify the Smart Sync state using the Dropbox icon overlays as explained here.

Opening online-only files

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

Downloading online-only files

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

Can I manage permissions of online-only folders?

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

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

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

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

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

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

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

Can I download a folder in the Boxcryptor drive?

Yes! To do this, click on **Boxcryptor** → **Download** in the context menu of the folder. This will download all files recursively. Note that this will only download the current state, files added remotely in the future will not be automatically downloaded.

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

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

Can I use Windows Search to find online-only files?

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

OneDrive Files On-Demand

OneDrive Files On-Demand is officially supported by Boxcryptor, since the new official release of the Windows 10 Fall Creators Update.

Google Drive File Stream

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

Box Drive

Box Drive is also officially supported by Boxcryptor.

Share Access to Files

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

What You Need to Know About Sharing Encrypted Files

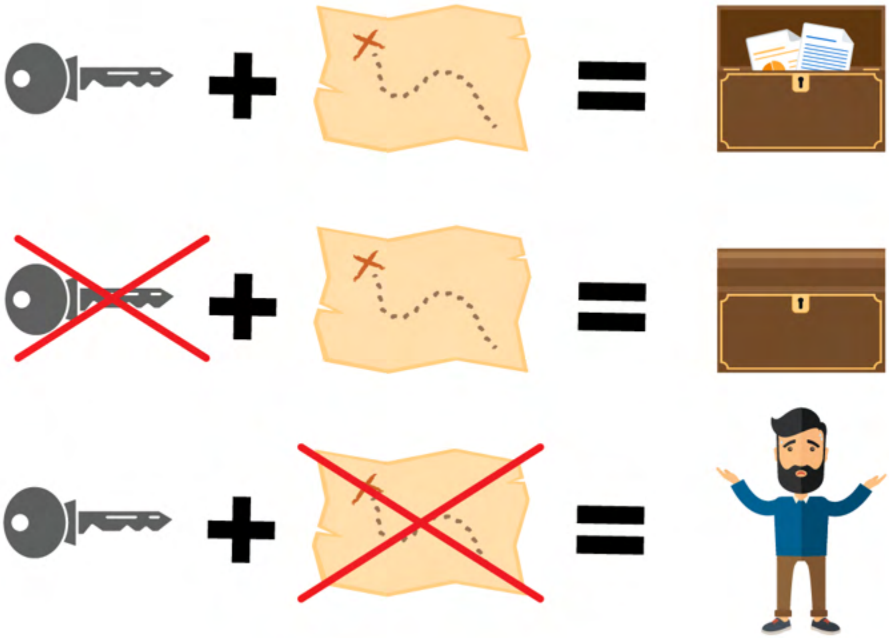
For understanding how the sharing of encrypted files works, it is helpful to understand how programs handle unencrypted and encrypted files.

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

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

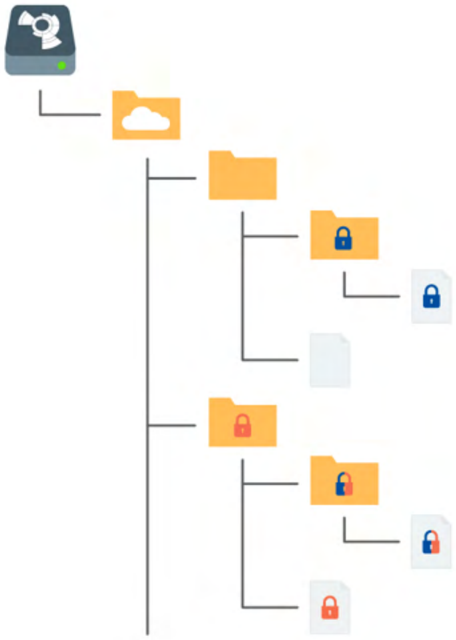
As a consequence, there are two steps necessary to share an encrypted file:

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



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

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



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

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

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

Share Files With Boxcryptor Users: Permissions

Using Boxcryptor, you can share encrypted files or folders with other Boxcryptor users.

> ℹ It is recommended, to not directly share an encrypted folder but rather place the encrypted folder in an unencrypted parent folder and share the unencrypted parent folder - especially when using filename encryption.

New files or folders (recommended)

1. Create a new unencrypted parent folder.
2. Create a new encrypted folder in the parent folder.
3. Right-click the **file or folder** → **Boxcryptor** → **Manage Permissions**.
4. Add the groups or users you want to share the file or folder with and apply the changes.
5. Copy the new files to the encrypted folder.
6. Share the **unencrypted parent folder** in your cloud provider.

Existing unencrypted files or folders

1. Create a new unencrypted parent folder.

2. Create a new encrypted folder in the parent folder.
3. Right-click the **encrypted folder** → **Boxcryptor** → **Manage Permissions**.
4. Add the groups or users you want to share the file or folder with and apply the changes.
5. Copy the existing unencrypted files to the encrypted folder.
6. Delete the existing unencrypted files.
7. Share the **unencrypted parent folder** in your cloud provider.

Existing encrypted folders

1. Create a new unencrypted parent folder.
2. Move the encrypted folder to the parent folder.
3. Wait until the changes have been synced by your cloud provider.
4. Right-click the **encrypted folder** → **Boxcryptor** → **Manage Permissions**.
5. Add the groups or users you want to share the file or folder with and apply the changes.
6. Wait until the changes have been synced by your cloud provider.
7. Share the **unencrypted parent folder** in your cloud provider.

> It is recommended to use groups in permission management as they can reduce the need for synchronization by your cloud provider when granting or revoking access to individual users. See Benefits of Groups for more information.

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. Find out how to use Whisply with Boxcryptor here.

Manage Groups

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

> 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.

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

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

These are the authentication methods you can choose from:

- **4-digit PIN code**: When set, you have to enter a 4-digit PIN code.
- **Password**: When set, you have to enter your Boxcryptor password.

> If you have logged into Boxcryptor via Single Sign-on, no Boxcryptor password is set and the password authentication option is therefore not available.

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

You can activate and set up the protection feature in the settings: **Boxcryptor tray icon** → **Settings** → **Security**.

Note: If an attacker gains access to your operating system, it is theoretically possible for him to modify the locally stored Boxcryptor settings in such a way that the protection feature can be circumvented. While this feature can help you better protect your encrypted data on your computer, it does not guarantee 100% security against sophisticated attackers with access to your operating system. We recommend to follow local device security best practices, to avoid such a situation.

Boxcryptor Settings

To access the Boxcryptor settings, right-click on the Boxcryptor icon located in the system tray and select Settings. Navigate to the **Advanced** tab to change the name of the Boxcryptor drive, its drive letter, autostart- and update settings, as well as filename encryption defaults.

The default settings are:

- Start with Windows
- Check for updates
- Hide files and folders starting with a dot

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

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

- **Enable Windows Search**: Give the Window Indexing service access to the Boxcryptor drive. More about it can be found here.
- **Enable recycle bin**: Deleting files will move them to trash, so that they can be restored if necessary.
- **Mount as fixed drive**: Even though the Boxcryptor drive is a virtual drive, this option will make it look and treated as a real drive.
- **Mount for all users**: System accounts will be able to access Boxcryptor.
- **Enable long path support** (Windows 7, 8, 8.1 only): Enables working with paths longer than 256 characters. Careful: This might cause problems and errors with other applications.

> ℹ Boxcryptor inherits the system-wide *Enable win32 long paths* setting shipped with Windows 10. Click **here** to learn how to enable it.

> ℹ Long path support depends on the characteristics of the underlying file systems. Older files ystems such as FAT32 (commonly used for USB sticks) *cannot* benefit from this setting.

- **Mount in Windows Mount Manager**: Adds the Boxcryptor drive to the Windows Mount Manager.
- **Hide files and folders starting with a dot**: Those files are generally meant to be hidden. This is enforced by this option.
- **Hide files and folders with names that cannot be decrypted**: If you cannot decrypt the names of the files and folders, you do not have access to them. Therefore, we hide them.
- **Hide OneDrive online file warning**: Boxcryptor cannot handle OneDrive's “on-demand” files. Enable this option to prevent warning messages from Boxcryptor when browsing folders with such files.
- **Auto detect removable drives**: Automatically mount USB sticks or external storages as Boxcryptor locations.
- **Auto detect network drives**: Automatically mount network drives as Boxcryptor locations.

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. Click ••• on the sign in screen.
2. Click on **Open key file**.
3. Select your existing key file.
4. Enter your password to sign into Boxcryptor.

Where Can I Delete my Account

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

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

You can delete your account when you sign in here.

Refer-A-Friend

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

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

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

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

Two-Factor Authentication

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

Authenticator App

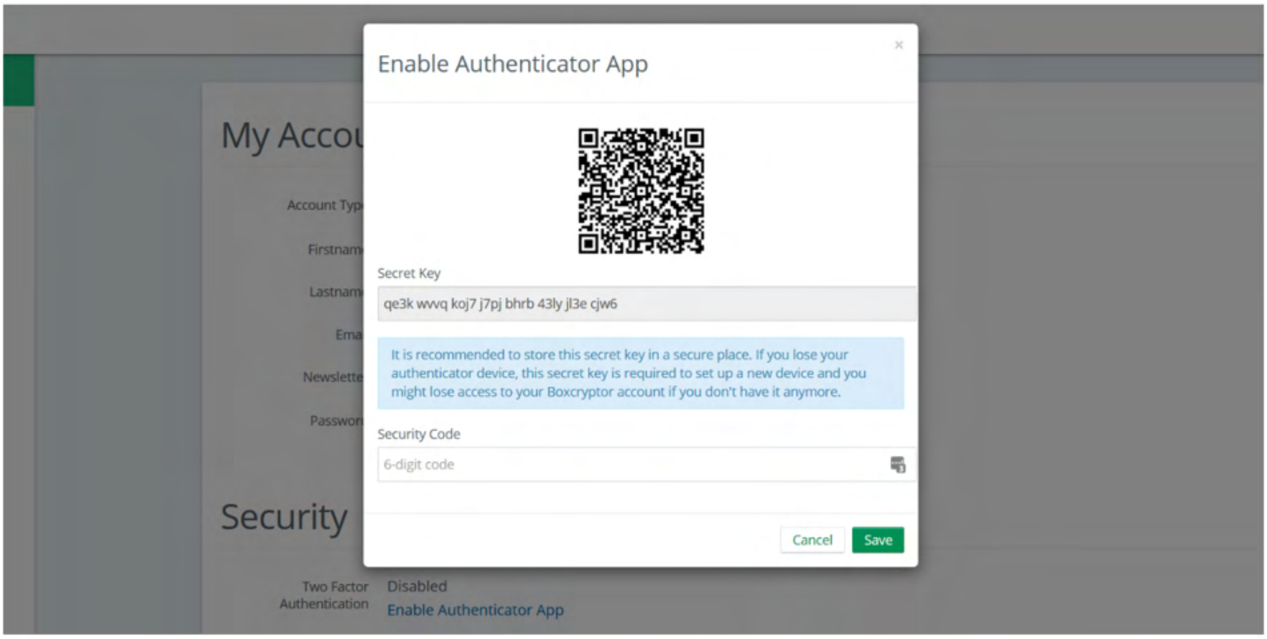
Authenticator apps use the Time-based One-Time Password algorithm (TOTP) to generate secure 6-digit code on your mobile device which have to be entered during authentication. To use it, **you need to install an Authenticator App** of your choice on your mobile device. Next, you need to configure both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

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

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

Read more about authenticator apps in our blog.

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



Enable Authenticator App

Secret Key

qe3k wvvq koj7 j7pj bhrb 43ly jl3e cjw6

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

Security Code

6-digit code

Two Factor Authentication: Disabled

Enable Authenticator App

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

Security Keys

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

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

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

Read more about security tokens on our blog

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

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

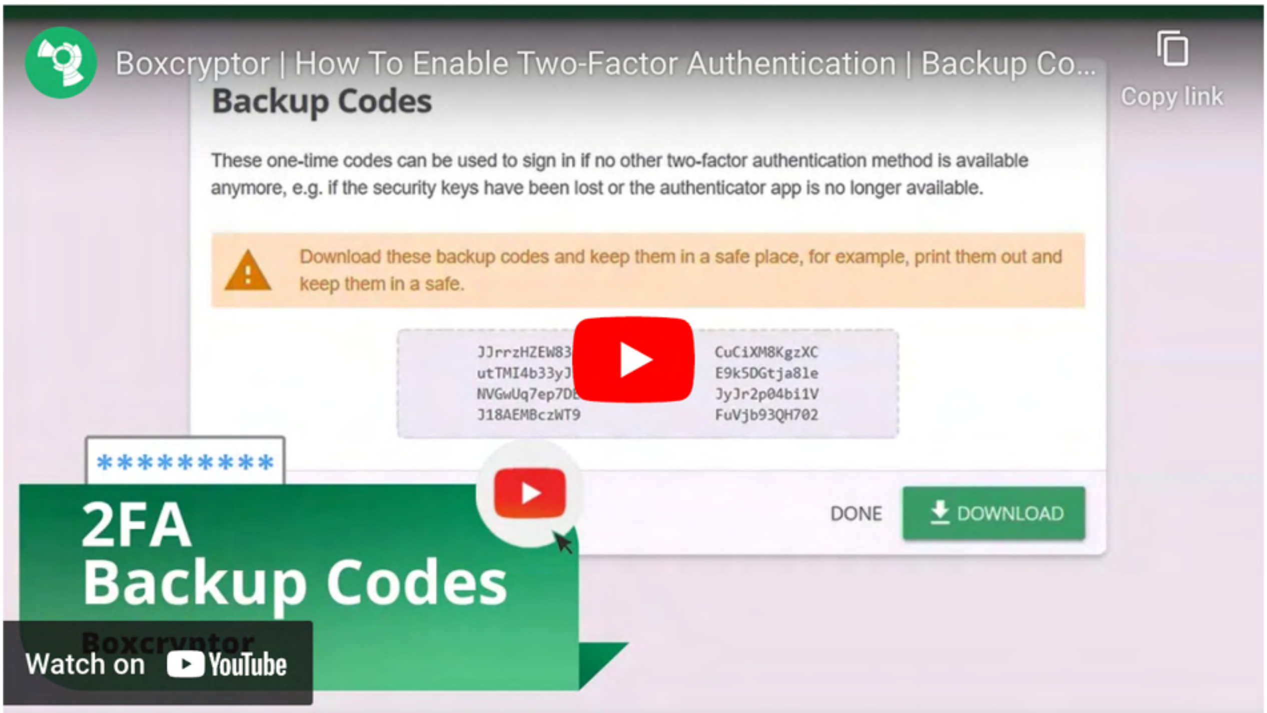
Limitations: Security keys are currently **not** supported on Boxcryptor for iOS, Boxcryptor for Android and Boxcryptor Portable. In these cases, you won't be able to sign in if 2FA is enabled. If accessing your account over boxcryptor.com, you need to use a modern browser.

Backup Codes

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

1. Sign in to boxcryptor.com.
2. Navigate to **Security**.
3. Click on **Two-factor Authentication -> Backup Codes**. (This option only is visible when at least

one second factor was added to the account.)
4. Now the newly generated backup codes are displayed at the screen.



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

Backup Codes

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

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

```
JJrrzHZEW83        CuCiXM8KgzXC
utTMI4b33yJ        E9k5DGtja8le
NVGwUq7ep7D        JyJr2p04bi1V
J18AEMBczWT9       FuVjb93QH702
```

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

2FA and the Protection feature

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

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

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

FAQ & Troubleshooting

Off-Migration Guide: Decrypt all Boxcryptor encrypted files

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

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

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

Migration Tips For Organizations

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

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

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

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

What happens if Boxcryptor goes out of business?

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

- Exported key file
- Boxcryptor installer file

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

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

I Cannot Install Boxcryptor

If the installation of Boxcryptor is not working, try the following:

Make sure .NET is installed correctly

- Install the Microsoft .NET Framework Repair Tool and follow its instructions.
- Install the latest .NET Framework.
- Restart your system.
- Install Boxcryptor.

Start Installation as Administrator

If this does not work, try starting the setup file manually with right-click → **run as Administrator**.

> This option is only available if the current Windows user profile is *not* an administrator profile.

Known Installation Issues

There are some known installation issues we are currently working on a fix for:

Error Code: 267

During the installation routine, the installer shows **Error Code: 267**.

This means that the user profile folder and the `Temp` folder within cannot be found by the installation routine. This seems to be tied to a prior Upgrade of Windows.

Workaround

Install Boxcryptor from a **different Windows User Profile**. If no other user account is at hand, temporarily create one here. Afterwards, the temporary profile can be deleted or disabled. Boxcryptor will now be usable via the original Windows account.

Missing DLL

During the installation routine, windows shows the following message:

> "There is a problem with this windows installer package. A DLL is required for this install to complete could not be run. Contact your support personnal or package vendor.

This is caused by antivirus software falsely flagging Boxcryptor as malicious software and thus preventing the installation.

Workaround

In order for Boxcryptor to be able to install properly, please make sure that antivirus software cant intervene. This can be done by:

- Deactivating the antivirus during installation
- Adding an exception rule for Boxcryptor to your antivirus
- Uninstalling your antivirus software and re-installing it after the Boxcryptor installation finished

If the installation still fails

If this does not help either, we need more feedback from the installer routine:

- Press the **Windows Key+R**, type `cmd` and press **Enter**.
- In the appearing window, type `cd <path to your installation file>`.
- Now enter `<installation file> /log log.txt`.

This command generates a log.txt file in the same folder as your installation file, containing important information about the failed installation. Look it through to find the reason for the failed installation, or send it to us.

My Screen Goes Black on Install

During installation we need to stop the Explorer to install the kernel driver explorer integration. Sometimes the Microsoft Software Installer (msi) fails to restore previous applications. In this case, you need to **manually restart the Explorer**.

- Open the Task manager (**Ctrl+Shift+Esc**).
- Click on **File** → **New task**.
- Type in "explorer" and hit enter to restore the explorer process.

I Cannot Update or Uninstall Boxcryptor

Sometimes deinstallation or an update of Boxcryptor fails with a request for the original installation file. This problem is caused by aggressive system enhancement apps.

To fix this, just **download the installer for your currently installed Boxcryptor version from our changelog** and provide it on request.

If this does not suffice, try Microsoft's deinstallation tool.

WebView2 Troubleshooting

Boxcryptor relies on Microsoft's **WebView2 (Evergreen) Runtime** for certain cases, such as **sign-in** and **Whisply integration**.

This runtime is included in Windows 11, Windows 10 installations that use Microsoft technologies such as Microsoft 365 will also have the runtime pre-installed.

Evergreen implies that Microsoft itself is responsible for keeping the runtime up-to-date, so developers can be sure that the latest features and security fixes are being deployed to client machines without having to update their apps.

However, there are scenarios where this automatic update does not work as expected, which can cause a version and compatibility discrepancy between the app's WebView2 module and the Runtime counterpart.

Boxcryptor tries to mitigate these scenarios by selectively disabling "newer" features of the Web View to at least keep the basic functionality available for the broader use.

We, however, **do not recommend keeping** your WebView2 Runtime in this **outdated** state, here are several approaches to fix it:

Install the latest version

Microsoft provides a downloader that should keep your WebView2 Runtime up-to-date, sometimes it help to just install it again. You can download it here.

Repair your current installation

In some scenarios, the installation was found in a corrupted state. To fix this, please go to your Apps and Features, search for `Microsoft Edge WebView2 Runtime` and select `Change` in the 3-dot menu. The installer will now appear with the option to `Repair` the current installation.

Boxcryptor is Using a Lot of CPU

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

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

Boxcryptor is Slow

An App is Slower Than Usual When Used With Boxcryptor

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

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

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

A Background Process is Causing High Load

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

Icons or the Context Menu are Not Shown

Boxcryptor uses its own channel to communicate with Explorer to display overlay icons or the context menu. If neither is displayed, this communication might not work correctly. There are three possible reasons for this:

You have started either Boxcryptor or the Explorer as another user

Correct this by opening the Task Manager (**Strg + Shift + Esc**), first selecting **Boxcryptor** → `Restart` and then **Explorer** →`Restart`.

There are too many Explorer processes running at the same time

Boxcryptor handles only a limited number of explorer processes simultaneously. Correct this by closing some **Explorer instances** via Task Manager (**Strg + Shift + Esc**).

All available spaces for the overlay symbols are occupied

Windows 10 has limited these to 9 free slots, so now all installed programs are fighting for them. Please take into account that every single symbol needs a free space.

The solution is to delete all unused entries:

1. Open the registry: **Windows key + R** → enter `regedit` → press ENTER
2. Navigate to this key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
3. Delete any keys that you think are no longer needed or that resemble "SkyDrive". (SkyDrive is the old OneDrive.)
4. Restart your system.

ℹ You are welcome to help alert Microsoft to this problem. Vote on it **here** via the Microsoft Feedback Hub.

How to Create a Debug Log

What is a Debug Log?

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

Does a Debug Log Contain Sensitive Data?

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

Which Information Does a Debug Log Contain?

The debug log captures the following information.

- User interaction such as button clicks and in-app navigation
- File operations (**including unencrypted filenames**)
- Current Boxcryptor settings
- Communication with our servers and your cloud provider(s)
- System information such as OS version or required frameworks
- Running programs
- Boxcryptor related windows event log reports
- User interaction and screenshots recorded with Windows Steps Recorder

How Do I Create a Debug Log?

1. Go to your Boxcryptor installation folder (`C:\Program Files (x86)\Boxcryptor`), → **double-click `Boxcryptor (Debug)`**.
2. Reproduce all steps that lead to the unexpected behavior.
3. Quit Boxcryptor by right-clicking on the tray icon → **Exit**.

A debug log archive (`Boxcryptor-<Timestamp>.seclog.zip`) is generated and saved to your desktop.

Additional System Information

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

1. Press **Windows** → write `msinfo32` → press **Enter**. The system information overview opens.
2. Now go to `File` → `Save` to export the information and send it to us, in addition.

On-the-fly logging

If you run into a problem and want to create a log straight away, you can tell Boxcryptor to start logging while it is already running:

1. Press **Windows Key+R** → type `bc.cmd` → press **Enter**. This opens an interactive Boxcryptor console.
2. Enter `debug` → press **Enter**.
3. Repeat the steps that lead to the problem.
4. Quit Boxcryptor by right-clicking on the tray icon → **Exit** or disable logging via the console: `debug --set-debug-mode=FALSE`.

Logging Boxcryptor during Windows Startup

1. Press **Windows Key+R** → type `bc.cmd` → press **Enter**. This opens an interactive Boxcryptor console.
2. Enter `debug --persistent` → press **Enter** to enable persistent logging.
3. Close the console window afterwards.

Boxcryptor will then notify you to disable it during startup.

Log filesystem accesses before execution

In rare cases it can be of interest to log accesses to the Boxcryptor drive before the file operation is carried out:

1. Press **Windows Key+R** → type `bc.cmd` → press **Enter**. This opens an interactive Boxcryptor console.
2. Enter `debug --eager-logging` → press **Enter** to enable persistent logging.
3. Close the console window afterwards.

Windows Steps Recorder

To better understand how the issue was produced, we use Microsoft's integrated Steps Recorder tool to take screenshots, record mouse clicks and track keyboard input.

You will feel a slightly degraded performance while the steps recorder is running.

Microsoft's Step Recorder will **not** record any of your keyboard input (it only marks an action as `keyboard input`). As long as you write your passwords in password fields (that obfuscate inputs), the screenshots won't show them.

To make sure everything was recorded to your wishes you can open and check the Steps recording (`Boxcrytor-<Timestamp>.seclog.zip\<Timestamp>-steps-recorder.zip\Recording_<Timestamp>.mht`) before sending the log to us.

Disable Steps Recorder

If you do not want to have any user interaction recorded, you can either delete the Steps recorder log from the output .zip file or start the debug mode without screen recording, with these steps:

1. Press **Windows Key+R** → type `bc.cmd` → press **Enter**. This opens an interactive Boxcryptor console.
2. Enter `debug --disable-steps-recorder` → press **Enter**.
3. Close the console window afterwards.

What Should I Do With my Debug Information?

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

Boxcryptor Crashes at Start

If Boxcryptor crashes when you start the software, it is likely that some component of the installation is at fault. To fix this, try the following steps:

- Uninstall Boxcryptor.
- Install the .NET-repairtool and follow its instructions.
- Install the latest .NET framework.
- Restart your system.
- Install Boxcryptor again.

Problems on Windows 7

Boxcryptor requires some components that may be missing when **automatic Windows Updates** are **disabled**.

Please turn on automatic Windows Updates (recommended) or download and install KB2999226 manually.

More information about this update can be found here.

I Cannot Connect to the Boxcryptor Servers

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

After the signing in, the App just returns to the sign-in screen

This may happen due to malconfigured SSL / TLS settings. Boxcryptor requires **TLS 1.2 or greater** for a secure client-server communication. On Windows 7 or some misconfigured computers, TLS 1.2 may not be enabled. Have a look at this Microsoft documentation to learn how to enable TLS 1.2. The most convenient way to solve the issue is the documentation attached Easy Fix Installer.

> We have seen incidences where some critial .NET updates where not installed on Windows 7 computers which are most likely causing connectivity issues even with enabled TLS 1.2 support. Microsoft offers some troubleshooting tips on each update, check out their respective landing pages.

Warning: This is no Secure Connection

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

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

Traffic inspection, techically speaking, is a **man-in-the-middle attack**. Therefore, it is important to make sure your system or internet connection is not compromised.

Working Offline

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

Proxy support

Boxcryptor inherits Window's Proxy settings, including authenticated proxies (which are authenticated on demand).

If Boxcryptor should bypass your proxy configuration, add following patterns to the exclusion list:

```
*.boxcryptor.com // for API access (required)
*.secomba.com // for update checks (optional)
```

Where can I download Boxcryptor Classic?

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

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

Download Boxcryptor Classic for Windows here:
https://www.boxcryptor.com/download/Boxcryptor_Classic_v1.7.409.131_Setup.msi *Supports Windows XP, Windows 7, Windows 8.1*

Download Boxcryptor Classic Portable for Windows here:
https://www.boxcryptor.com/download/BoxcryptorClassicPortable_1.6.402.92.zip *Supports Windows XP, Windows 7, Windows 8.1*

Advanced Client Configuration

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

How to manage the application configuration file

Boxcryptor's configuration file **`Boxcryptor.exe.config`** is located in the Boxcryptor installation folder (**`%PROGRAMFILES(x86)%\Boxcryptor`**). To make modifications to this file, open it in a text editor.

> ⚠ Changes in **`%PROGRAMFILES(x86)%`** require administrative permissions. If using the default text editor (`Notepad.exe`), it must be run as administrator to successfully save modifications. (**Windows Key** + type "Notepad" -> right-click on the texteditor in the search result -> **Run as Administrator**)
> Also make sure that the result is saved as a `.config` file, as some Editors may append `.txt`.

The application configuration file is a XML based configuration with following format:

```
<configuration>
  ...
  <appSettings>
    <add key="KEY" value="VALUE" />
  </appSettings>
  ...
</configuration>
```

To change any setting defined by a **`key`**, change the associated **`value`** string.

ℹ The Configuration file is loaded when Boxcryptor is starting. If Boxcryptor is running when you modify a the config, you have to restart Boxcryptor in order for the change to be applied.

⚠ Updating Boxcryptor may revert the configuration file. Make sure to create a backup of your configuration.

List of application settings

- **EncryptByDefault** (default `false`): New files created by applications in unencrypted directories will be written encrypted by default.
- **AlternateDataStreamSupport** (default `true`): Support for alternate data streams. Note that ADS support is only enabled if all enabled Boxcryptor locations do support this feature.
- **EncryptDialogIncludedProcesses**: A comma-separated list of processes which will trigger the "Do you want to encrypt" Dialog when creating files in unencrypted directories.
- **SupportedBackupProcesses**: A comma-separated list of processes which that will receive backup-optimized file system I/O such as early downloading on-demand files.
- **CreateLogOnCrash** (default `true`): Create log file in `%LOCALAPPDATA%\Boxcryptor\Crash Logs` upon crash.
- **ProcessNamesPreventingShutdownOnSessionEnd**: A comma-separated list of all processes that need to be closed before Boxcryptor closes on session end to prevent data loss on files open via the Boxcryptor volume.
- **DisableAutomaticUpdates** (default `false`): Prevent automatic updates and also suppress any update notifications.
- **DisableExplorerQuickAccess** (default `false`): Disable the creation of the Boxcryptor quick access icon in the Windows Explorer's navigation pane.
- **CustomSettingsPath** (default `""`): A custom path where Boxcryptor stores it's user settings. Can contain environment variables. See Teams/Deployment/Custom Settings location for more information.
- **EnableTerminalEnvironmentMode** (default `false`): Predefines and restricts certain Boxcryptor settings to be compatible to thin clients (Terminal / Citrix Server).
- **RefreshUserPeriodMs** (default `15000`): Defines the period in milliseconds in which the client synchronizes with the Boxcryptor servers.
- **DisableInitialTutorialAndTour** (default `false`) Permanently deactivates the automatic display of the tutorial and the introduction.
- **WebView2CommandLineParameters** (default `""`): Provides the ability to transfer command line parameters to the WebView2 web rendering engine.
- **TryReconnectRemoteLocationsOnStartup** (default `true`) Attempts to reconnect disconnected network locations (SMB and WebDAV) at startup. Might show a user authentication dialog.

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.

How to use Windows Search / Cortana

To make use of Windows Search / Cortana to search within Boxcryptor encrypted files, following advanced settings are required:

- `Enable Windows Search`
- `Mount as fixed drive`
- `Mount for all users`
- `Mount in Windows Mount Manager`

Afterwards, the Boxcryptor drive has to be addes as a location in the Windows Indexing Options.

Sometimes changing the settings requires **restarting the computer** in order for the Boxcryptor drive to show up as an available location in the Indexing Options.

Adding the Boxcryptor drive to the Windows Search Index can result in severe CPU load and performance degradation as Windows is indexing all files in the Boxcryptor drive. In addition, content that is actually encrypted can end up in the unencrypted Windows search index.

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.

Incompatibility with Bitdefender

We have recently received frequent customer feedback that the Boxcryptor drive is no longer available after a few hours of operation or after the system has been on standby, or that Boxcryptor itself is no longer running.

In the Windows Event Viewer → Windows Logs → Application these crashes are listed as `Application Error` as follows:

```
Faulting application name: Boxcryptor.exe, Version: 2.XX.XXXX.0, time stamp:
Faulting module name: KERNELBASE.dll, version: X.XX.XX.XX, time stamp: [...]
Exception code: 0xe0000008 | 0xe0434352
[...]
```

Alternatively, errors about `System.OutOfMemoryException` can also be listed under `.NetRuntime`.

Another indication of this crash is a **red Boxcryptor tray icon** and an SSL Notification.

After some intensive research and evaluation of various error logs, we were able to identify **Bitdefender** as the cause of the problem.

Possible Workarounds

⌄ Bitdefender for Home

The only remedy here for the time being is to restart Boxcryptor in the event of a crash, to disable **Advanced Thread Defense** in Bitdefender or to **uninstall Bitdefender** alltogether and restart the system. When doing this, be aware that Bitdefender may install several individual software components.

Bitdefender for Business

In Bitdefender for Business solutions (e.g. Gravity Zone) there is an option to add `Boxcryptor.exe` to a exclusion list for various modules (On-Demand, On-Access, ATC/IDS and Ransomware).

We have already contacted Bitdefender and will publish the latest findingshere and in our Community.

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

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

Ways to recover access to your account:

Re-apply the secret key from your initial setup

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

For reference, the secret key looks similar to:

> mzwe wocd mj3d qr3f njjw g2cm grqw cvli

Use a device code

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

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

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

Use a backup code

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

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

None of the above methods apply

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

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

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

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

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

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

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

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

Invalid Authenticator App Codes

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

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

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

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

About

Maintenance Window

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

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

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

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

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

Changelog

Version 2.55.2774 (2022-11-08)

- Fixed: Saving issue with Office on network drives and removable storages
- Minor bug fixes and improvements

Version 2.54.2765 (2022-11-02)

- Added: Option to enable Windows Search explicitly
- Added: Support for location policy wildcards
- Improved: Faster download for OnDemand files
- Improved: WebDAV support
- Improved: Reconnect handling for disconnected network locations
- Improved: locations with the same foldername can now be added
- Removed: pCloud auto-detection
- Fixed: Issues with Whisply links and auto-detection for Google Drive
- Fixed: Incompatibility with Box Drive
- Minor bug fixes and improvements

Version 2.53.2568 (2022-07-27)

- Fixed: Incompatibility with Volume Shadow Copy Service (VSS)
- Fixed: File handles are closed with significant delay

- Changed: Plaintext files and folders no longer show a white overlay icon
- Changed: Upgraded CBFS Connect to v20.0.8181
- Minor bug fixes and improvements

Version 2.52.2484 (2022-05-27)

- Fixed: Cut and paste of folders from the Boxcryptor drive to another volume results in empty target folder
- Fixed: Incompatibilities with old or broken WebView2 installations
- Minor bug fixes and improvements

***Note:** This version contains a known incompatibiliy with Windows Volume Shadow Copy Service (VSS). If you encounter issues with VSS, temporarily enable **Mount for all users** and **Mount with Windows Mount Manager** in the Advanced Settings or quit Boxcryptor to use VSS.*

Version 2.51.2468 (2022-05-19)

- New: Device Codes as second factor for authentication on other devices
- New: Support for GMX Cloud and Web.de Online-Speicher
- Fixed: Compatibility issues with Windows Search
- Fixed: Compatibility issues with Recycle Bin on Windows 11
- Fixed: Google Drive shortcuts to filename encrypted folders
- Improved: Microsoft Teams channel detection
- Changed: Dropped Support for Windows 7, Windows 8 and Windows 8.1
- Changed: Upgraded from CBFS Connect 2017 to CBFS Connect 2020 (v20.0.8132)
- Changed: Use WebView2 instead of Chromium Embedded Framework
- Changed: Updater now checks daily for new updates
- Removed: Creation of new local accounts. Existing local accounts including key exports are not affected by this change.
- Improved: Greatly reduced MSI installer size
- Minor bug fixes and improvements

ⓘ This update requires a computer reboot

***Note:** This version contains a known incompatibiliy with Windows Volume Shadow Copy Service (VSS). If you encounter issues with VSS, temporarily enable **Mount for all users** and **Mount with Windows Mount Manager** in the Advanced Settings or quit Boxcryptor to use VSS.*

Version 2.50.2196 (2022-01-31)

- New: Support for new MagentaCLOUD Sync Client
- Changed: App Protection will now reset app on consecutive failed unlock attempts
- Improved: Network location performance and stability
- Minor bug fixes and improvements

ⓘ This is the last Boxcryptor version supporting **Windows 7 / 8 / 8.1**.

Version 2.49.1965 (2021-10-14)

- New: Windows 11 support
- Fixed: Microsoft Teams private channels are not correctly auto-detected
- Fixed: Multiple mirrored Google Drive accounts are not correctly auto-detected
- Changed: Temporarily disabled recycle bin support on Windows 11 due to compatibility issues
- Minor bug fixes and improvements

Version 2.48.1906 (2021-09-22)

- Added: Support for new Google Drive client
- Improved: Network location performance and startup time
- Minor bugfixes and improvements

Version 2.47.1752 (2021-06-30)

- Fixed: Connection issues on Windows 7
- Fixed: Driver installation could fail when upgrading from specific version
- Improved: DPI awareness
- Minor bugfixes and improvements

Version 2.46.1654 (2021-05-31)

- New: On-demand files support for OwnCloud, NextCloud and iCloud Drive
- Fixed: Cannot delete files in Azure Files locations
- Fixed: Cannot create Whisply links for files in OneDrive shared drives
- Fixed: Do not use drive letters of disconnected network shares
- Fixed: Google Drive must be re-linked after some time
- Minor bugfixes and improvements

Version 2.45.1556 (2021-03-29)

- New: Microsoft Teams integration
- New: Terminal Server mode
- Changed: Upgraded CEF to v88.2.90
- Changed: Upgraded .NET Framework to 4.7.2
- Improved: Performance and stability regarding network locations
- Minor Bug fixes and improvements

For security reasons, Boxcryptor requires **TLS ≥ 1.2** for client-server communication, which must be activated manually under **Windows 7**.

Version 2.44.1485 (2021-02-23)

- Fixed: Google Drive (File Stream) detection did not work for new installations
- Fixed: Boxcryptor installation directory could change during update
- Fixed: Office sometimes failed to open online-only files
- Improved: Dropbox Smart Sync support
- Minor Bug fixes and improvements

Version 2.43.1441 (2021-02-03)

- Fixed: Compatibility with Google Drive (File Stream) v45.0.12.0
- Fixed: Fixed rendering issues with Intel Graphics drivers
- Changed: pCloud auto-detection is now restricted to the sync folder
- Minor Bug fixes and improvements

Version 2.42.1333 (2020-12-10)

- Changed: Spideroak auto-detection is now restricted to the SpiderOak Hive folder
- Fixed: Crashes related to recent Windows Updates
- Fixed: Installing updates when using a proxy
- Bug fixes and improvements

Version 2.41.1246 (2020-10-07)

- New: Google Shortcut support
- Improved: Shortcut (.lnk) file support
- Improved: Compatibility with various backup solutions
- Improved: HiDrive auto detection of public folders
- Changed: Sign-out is now part of the account settings
- Fixed: Administrators could not change permissions to other groups using the Master Key
- Minor bug fixes and improvements

Version 2.40.1216 (2020-06-04)

- New: Dark Mode Support for Windows 10
- Changed: Upgraded CBFS Connect to v2017.0.27
- Changed: Enforced password length restrictions for local accounts
- Fixed: Stability issues on network drives
- Bug fixes and improvements

> ⓘ This update requires a computer reboot

Version 2.39.1135 (2020-04-16)

- New: Disable Whisply policy
- Added: LeitzCloud auto detection
- Added: IONOS HiDrive auto detection
- Fixed: Saving and moving new files could could lead to file corruption on network locations
- Fixed: Saving files in Adobe Acrobat DC on network locations could fail
- Fixed: Storage Authentication lost after Boxcryptor restart when using Whisply integration with Dropbox Business
- Bug fixes and improvements

Version 2.38.1080 (2020-02-10)

- Added: More folder icons for providers
- Changed: Boxcryptor now always uses System proxy settings

- Changed: Upgraded CBFS Connect to v2017.0.24
- Changed: Removed SSL Pinning in favor of certificate transparency
- Improved: Startup performance
- Fixed: Issues related to saving Office files to network locations
- Fixed: Incompatibility with Box Drive
- Fixed: Whisply integration could get unlinked under certain conditions
- Fixed: Boxcryptor drive could be accessed by other windows user account when mounted as network drive
- Bug fixes and improvements

This update requires a computer reboot

Version 2.37.1057 (2019-10-24)

- Added: Official support for Windows 10 1909
- Added: auto detection for various Amazon S3 clients:
  - CloudBerry Drive
  - Mountain Duck
  - ExpanDrive
- Added: Egnyte Drive and Egnyte Sync auto detection
- Fixed: Security Keys required Boxcryptor running as administrator
- Bug fixes and improvements

Version 2.36.1046 (2019-09-02)

- Improved: better Performance and less memory usage
- Fixed: Some Dropbox online-only files could not be opened
- Fixed: Some Google Drive File Stream files could not be opened
- Fixed: Boxcryptor sometimes hangs when running the debug mode
- Fixed: Incompatibility with some PDF annotators
- Bug fixes and improvements

Version 2.35.1033 (2019-06-24)

- Added: pCloud auto detection
- Improved: Performance improvements (esp. when using network drives)
- Improved: Better verification when linking a cloud storage account
- Changed: Linking Google Drive or Google Drive Filestream will now open an external browser window
- Changed: Updated CBFS Connect to v2017.0.18
- Fixed: Dropbox does not always sync copied tiny encrypted files
- Fixed: Cannot open encrypted folders if the folder key cannot be accessed (e.g. due to missing filesystem permissions)
- Fixed: Local account does not correctly resolve groups
- Fixed: Yandex.Disk auto detection
- Fixed: Nutstore auto detection
- Removed: Group Management (now available at boxcryptor.com)
- Removed: Edit Account (now available at boxcryptor.com)
- Removed: Cuda Drive (service does not exist anymore)

- Removed: Cubby support (service does not exist anymore)
- Minor bug fixes and improvements

ⓘ This update requires a computer reboot

Version 2.34.995 (2019-03-20)

- Added: SharePoint Online & 2019 auto-detection
- Added: Alternate data streams support can be disabled via app.config
- Changed: Allow internet links in OneDrive
- Changed: Removed Master Key Generation because Master Key setup is now available at boxcryptor.com
- Fixed: Saving files in Google Drive File Stream v29.1.85.2056 can fail under certain conditions
- Fixed: Saving files in OneDrive can fail under certain conditions
- Fixed: Saving Office files in network drives can fail under certain conditions
- Fixed: Deleting files in network drives can fail under certain conditions
- Fixed: Windows Explorer preview pane interferences with Boxcryptor
- Fixed: Regular files matching Excel temporary filename pattern are excluded from sync
- Fixed: License keys are sometimes not correctly parsed
- Fixed: Groups in exported key files are not correctly parsed
- Fixed: Boxcryptor crashes if a location policy with a macOS-only value exists
- Minor bug fixes and improvements

Version 2.33.933 (2019-01-25)

- Fixed: Google Drive File Stream related app crash
- Fixed: OneDrive OnDemand download timed out sometimes
- Minor bug fixes and improvements

Version 2.32.910 (2018-12-10)

- Improved: Performance improvements (up to 100% in certain benchmarks)
- Fixed: Access denied error when flushing a file on network drives under certain circumstances
- Fixed: Files cannot be decryped when being offline under certain cirumstances
- Fixed: Long path support
- Fixed: Regression performance degradation on network drives
- Changed: Upgrade BouncyCastle to v1.8.4
- Minor bug fixes and improvements

Version 2.31.870 (2018-10-19)

- Changed: Upgraded CBFS Connect to v2017.0.10
- Changed: Offline/Online Notifications are now removed in favor of an icon state
- Improved: Handling for internet links in a folder (Google Docs, OneNote Notebooks, ...)
- Improved: Errors when processing many files can now be skipped
- Improved: OneDrive OnDemand files compatibility
- New: Debug log will also generate a Steps recorder log
- Fixed: Whisply integration for OneDrive Germany
- Minor bug fixes and improvements

This update requires a computer reboot

Version 2.30.833 (2018-08-16)

- Improved: Proxy support
- Fixed: Date modified is not preserved when copying files with alternate data streams
- Minor bug fixes and improvements

Version 2.29.799 (2018-05-24)

- Updated: Privacy Policy
- Fixed: Google Drive File Stream
- Fixed: App could start multiple times
- Minor bug fixes and improvements

Version 2.28.797 (2018-05-09)

- Fixed: Installation rollback issues with the latest Windows 10 update

Version 2.27.795 (2018-05-04)

- Updated: Privacy Policy
- Minor bug fixes and improvements

Version 2.26.784 (2018-04-23)

- Changed: Removed ability to move OneDrive on-demand files to the recycle bin again due to a bug in Windows which can only be fixed by Microsoft.
- Fixed: OneDrive on-demand files can now be moved to the recycle bin
- Fixed: Copying files in Explorer sometimes silently fails and does nothing
- Fixed: Files are always renamed on name collisions in copy or move via Explorer
- Fixed: Copying read-only files with alternate data streams fails
- Fixed: Opening alternate data streams sometimes fails
- Minor bug fixes and improvements

Version 2.25.777 (2018-04-06)

- Added: Windows 10 1803 support
- Added: Dropbox Team Spaces support
- Added: On-demand files are downloaded before they are copied or moved in Windows Explorer
- Added: Option to disable auto-updates via app.config
- Improved: Various installer improvements
- Changed: Upgraded from CBFS v6 to CBFS Connect v2017.0.5
- Minor bug fixes and improvements

Version 2.24.747 (2018-02-28)

- Added: Downloading multiple on-demand files
- Fixed: Opening files can fail with Google Drive File Stream version 25.157.165.2150 and newer

- Fixed: Cannot copy files with alternate data streams to a location in the Boxcryptor drive which resides on a volume with does not support alternate data streams. The Boxcryptor drive only advertises alternate data stream support if all enabled locations reside on volumes with alternate data stream support (e.g. NTFS file systems)
- Minor bug fixes and improvements

Version 2.23.726 (2018-02-13)

- Fixed: Autostart settings are sometimes overwritten after update
- New: ownCloud and Nextcloud auto detection
- New: Plex Media Server support
- New: Alternate data stream support
- Updated: Certificates used for certificate pinning
- Bug fixes and improvements

Version 2.22.706 (2017-12-13)

- Fixed: Some folders cannot be encrypted or decrypted
- Fixed: Tray icon disappears on re-mount
- Minor bug fixes and improvements

Version 2.21.691 (2017-12-04)

- Fixed: Locations settings are lost after restart
- Fixed: On-Demand notifications are not shown for OneDrive
- Fixed: Cannot rename folder on NAS location sometimes
- Fixed: Editing PDFs fails in FileCenter software
- Fixed: Windows search indexing triggers on-demand file downloads
- Minor bug fixes and improvements

Version 2.20.680 (2017-11-22)

- New: Google Drive File Stream support
- New: Encryption Required policy
- Minor bug fixes and improvements

Version 2.19.658 (2017-10-10)

- New: Prevention of data loss for unsaved changes at Windows shut down
- Minor bug fixes and improvements

Version 2.18.646 (2017-09-21)

- New: Experimental support for the new Box Drive client
- Minor bug fixes and improvements

Version 2.17.635 (2017-08-07)

- Fixed: HiDrive auto detection now works for latest HiDrive client update
- Fixed: Dropbox Smart Sync compatibility on Windows 8.1
- Minor bug fixes and improvements

Version 2.16.629 (2017-08-01)

- Major redesign of the user interface for creating accounts and signing in
- New: Experimental support for OneDrive Files On-Demand
- New: Boxcryptor quick access in Windows Explorer
- New: Nutstore auto detection
- New: Disallow to manage permissions policy
- Improved: Yandex auto detection
- Improved: Faster update process
- Improved: Explorer integration stability
- Fixed: Boxcryptor could crash on Windows 7 with stylus support due to .NET bug
- Minor bug fixes and improvements

Version 2.15.578 (2017-06-13)

- Added: OneDrive for Business Germany support
- Fixed: Google Drive authentication
- Fixed: Disabling Boxcryptor autostart sometimes did not work
- Minor bug fixes and improvements

Version 2.14.564 (2017-05-12)

- Improved: App stability
- Minor bug fixes and improvements

Version 2.13.560 (2017-05-06)

- Improved: App stability
- Fixed: Multiple crash logs were created
- App protection usability improvements

Version 2.12.553 (2017-04-24)

- Fixed: Password protection was always enabled when updating from versions older than 2.11.550

Version 2.11.550 (2017-04-18)

- Added: Additional PIN protection and reworked password protection (Learn more)
- Added: Support for Whisply with OneDrive for Business
- Improved: Filesystem stability (e.g. when downloading files via Chrome)
- Minor bug fixes and improvements

Version 2.10.542 (2017-04-04)

> Likewise to Boxcryptor for macOS, Boxcryptor permissions are not checked when browsing into encrypted folders anymore. When any action is performed in an encrypted folder, permission checks still apply.
> Checking permissions when browsing into an encrypted folder was only a "convenience" feature because the user could always browse into the folder directly in the location and the new behavior reflects this possibility also in the Boxcryptor drive.

- Added: Support for Dropbox Smart Sync (Learn more)
- Improved: The Boxcryptor context menu in Windows Explorer is now capable to operate on multiple selected files / folders
- Improved: Whisply links can now be created for folders and also for unencrypted files which will automatically be encrypted first. The overall maximum of 5 files per Whisply link still applies.
- Improved: Filesystem stability
- Fixed: Boxcryptor could crash when USB thumb drives were removed
- Minor bug fixes and improvements

Version 2.9.526 (2017-03-09)

- Improved: Network drive handling
- Improved: Context menu performance
- Improved: Handling for .bc files including file association with Boxcryptor
- Added: Permission warning when trying to decrypt files without Boxcryptor access
- Fixed: Sometimes account creation could fail
- Minor bug fixes and improvements

Version 2.8.505 (2017-02-09)

- Minor bug fixes and improvements

Version 2.7.503 (2017-02-06)

- Added: Automatic upgrade of encrypted file format if required
- Fixed: Temporary SQlite files have not always been deleted
- Fixed: Google Drive authentication could fail
- Fixed: With 7zip installed, files where copied to the Boxcryptor drive instead of moved
- Improved: Better recovery for network drive locations
- Minor bug fixes and improvements

Version 2.6.493 (2017-01-16)

- Added: HubiC auto detection
- Improved: OneDrive for Business auto detection
- Fixed: Authentication for Whisply integration
- Improved: .Net Framework detection for Windows 7
- Minor bug fixes and improvements

Version 2.5.484 (2016-12-20)

> **Windows 7** users need the .NET Framework 4.5.2 to get Boxcryptor to run. You may find the download *here*.

- Added: Amazon Drive auto detection
- Updated: Data Protection Policy
- Fixed: Filename encryption settings did not show correctly
- Minor bug fixes and improvements

Version 2.4.482 (2016-12-16)

> This version does **not** support **Windows XP** and **Windows Vista** anymore. As these old versions are not supported by Microsoft anymore, we recommend affected users to update their operating system to a newer version as soon as possible in order to stay safe.

- Added: Office 2013+ Integration
- Added: In-app network drive authentication
- Added: Support for custom certificate pinning allowing to use Boxcryptor in networks with SSL interception performed by e.g. anti-virus software or proxy servers
- Improved: Boxcryptor can be used in offline mode when a secure connection to the Boxcryptor servers cannot be established due to SSL interception and custom certificate pinning is not enabled
- Improved: Various performance improvements, especially when using MS Office
- Improved: Better drive letter in use detection
- Improved: Updated CBFS to v6.1.184
- Changed: The patch number has been removed from the versioning scheme so that it has been changed from Major.Minor.Patch.Build to Major.Minor.Build. New releases will always increment the Minor number instead of the patch number
- Changed: Dropped support for Windows XP and Windows Vista
- Updated: Certificates used for certificate pinning
- Fixed: Sometimes specific locations could not be added
- Various other bug fixes and improvements

Version 2.3.415.455 (2016-09-26)

- Fixed: Sometimes the update notification did not show
- Improved: Apply button on manage permission page only enabled when there are changes
- Improved: Resolving file hiding conflicts between files and folders
- Improved: Tutorial
- Minor improvements and bug fixes

Version 2.3.413.448 (2016-09-08)

- Fixed: OneDrive for Business detection
- Improved: Boxcryptor now uses the Windows UI language
- Minor improvements and bug fixes

Version 2.3.411.446 (2016-09-01)

- Fixed: Icon Overlay conflict with OneDrive
- Due to new limitations in Windows 10 and the latest OneDrive update our overlay icons might have been lost. We decreased the number of used icons now to avoid further issues.
- Added: New location picker
- More flexible location picker let users even add locations manually via an address bar.

Version 2.3.409.438 (2016-08-25)

- Added: Command Line option to change default settings path
- Added: Duplicate file hiding resolving
- Files and folders hiding other items can now be automatically renamed.
- Added: Warning for bad encryption / decryption workflow

- Users will now be informed when they decrypt and re-encrypt folders unnecessarily
- Fixed: Encryption forbidden dialog could not be closed
- Fixed: Settings could get resetted when USB thumbsticks where removed
- Minor improvements and bug fixes

Version 2.3.407.426 (2016-08-09)

- Improved: Installer (silent installation improvements, removed shortcut creation on update)
- Fixed: Whisply integration for Google Drive
- Minor improvements and bug fixes

Version 2.3.405.406 (2016-07-27)

- Added: Login with Command Line Interface (experimental)
- Fixed: Explorer crashing under certain circumstances

Version 2.3.403.402 (2016-07-21)

- Added: Check permissions for folders
- Check Boxcryptor permissions directly via the Manage Permissions Window.
- Fixed: Credentials lost with bad internet connection
- Fixed: Share Whisply link with local account
- Fixed: Locations are sometimes selected automatically when trying to add new ones
- Improved: Invitation of new Boxcryptor users to groups and when managing file permissions
- Minor improvements and bug fixes

Version 2.3.401.400 (2016-07-07)

- Added: Whisply integration
- Transfer files securely end-to-end encrypted in Dropbox, OneDrive and Google Drive with a simple link.
- Added: Sync status in icon overlays
- See directly in Boxcryptor if a file is currently being synced, if it is synced or if there is a sync problem.
- Added: Command Line Interface (experimental)
- Automate your Boxcryptor deployment and configure Boxcryptor using a simple command line interface without having to use the GUI.
- Improved: Faster sign in
- Improved: No internet connection required to work in folders shared permissions
- Improved: Updated to CBFS v6.1.180
- Improved: Boxcryptor is not mounted as network drive on Windows 10 anymore
- Minor improvements and bug fixes

Version 2.2.423.322 (2016-04-04)

- Improved: Master key support with exported key files (reexport needed)
- Fixed: Some locations could not be enabled in certain circumstances
- Minor bug fixes and improvements

The v2.2.x versions are the last versions with Windows XP & Windows Vista support. They are not actively supported by Microsoft anymore and we strongly encourage every user who is still using any of these old, unsecure operating systems to upgrade to a newer, secure version.

Version 2.2.421.309 (2016-03-09)

- Fixed: Removed A:\ and B:\ being selectable as drive letter due to inconsistent behaviour
- Added: Whitelist locations company policy
- Added: Required locations company policy

Version 2.2.419.277 (2016-02-23)

- Added: MagentaCloud auto detection
- Improvement: Auto detection for newer Dropbox client version
- Minor bug fixes and improvments

Version 2.2.417.266 (2016-02-03)

- Fixed: Windows 10 drive icon not being removed
- Improved: Exclude system files like Thumbs.db or .DS_Store from sync
- Feature: Support OneDrive for Business NextGen Client
- Improved: Cubby auto detection
- Minor bug fixes and improvements.

Version 2.2.415.246 (2015-12-22)

- Fixed: Under certain circumstances, encrypted files get damaged after granting permissions to more than 5 or 6 users or groups (error message: "Found invalid data while decoding"). If you are affected, please contact us at support@boxcryptor.com for information how to repair those files.
- Minor bug fixes and improvements.

Version 2.2.413.244 (2015-12-16)

- Added: Auto-detection for LiveDrive.
- Changed: Renaming a plain text file or folder in an encrypted folder does not automatically encrypt it anymore.
- Fixed: The file name of an encrypted Office document does not keep its encryption setting if the document is saved within a plain text folder.
- Fixed: Sporadical drive deadlock and/or very poor performance when saving Office documents on network shares.
- Fixed: Changing the case of a file or folder name deletes it under certain circumstances.
- Fixed: LiveDrive syncing causes Boxcryptor to create lots of files.
- Minor bug fixes and improvements

Version 2.2.411.228 (2015-10-19)

- Fixed: Minor bug fixes

Version 2.2.409.226 (2015-10-14)

- Added: Auto-detection for CudaDrive
- Fixed: Driver incompatibility with Strato HiDrive (and other CBFS-based drives).

Version 2.2.407.225 (2015-10-07)

- Added: Advanced option to disable auto-detection for removable and network drives
- Added: Support for Office 2016
- Improved: Updated CBFS to v5.1.164
- Fixed: Location settings are lost on restart

Version 2.2.405.221 (2015-09-28)

- Fixed: Crash when pressing Ctrl + any key not related to copy/paste on password field
- Fixed: Added support for single letter TLDs (e.g "q.com")
- Fixed: User couldn't access a location sometimes

Version 2.2.403.216 (2015-08-28)

- Improved: Updated CBFS to v5.1.163.
- Fixed: Some files could not be correctly read.
- Fixed: Mounting the drive as network drive failed if the drive or machine name is empty.
- Fixed: Could not enable custom locations.

Version 2.2.401.210 (2015-08-18)

- Added: Support for Windows 10
- Added: Auto-detection for Copy.com Sync
- Improved: Updated CBFS to v5.1.162
- Improved: Copy or move operations with multiple files now only ask once whether it should be encrypted instead of multiple times for every file.
- Fixed: Cannot checkout Git repositories on the Boxcryptor drive.
- Fixed: Executing the command "vssadmin.exe list shadowstorage" finished with internal error.
- Fixed: Creating a directory did ignore attributes (directories have always been created with default attributes).
- Fixed: Use "Removable Disk" placeholder for removable disk location name if it would be empty.
- Various other bug fixes and improvements.
- Known Issues:
- - A folder within the Boxcryptor drive cannot be added as a location in the Windows Photos app.
- - Due to a driver incompatibility in CBFS v5.1.162, Boxcryptor cannot access locations which are also a virtual drive using CBFS. Due to this limitation, Strato HiDrive is currently not supported in this version. If you want to use Boxcryptor with Strato HiDrive, please do NOT update to this version and instead use Boxcryptor for Windows v2.1.417.123 which is still using CBFS v4. We are working with the vendor of CBFS to resolve this issue as soon as possible. UPDATE: The driver incompatibility has been resolved in v2.2.409.226.

Version 2.1.417.123 (2015-06-29)

- Fixed: Files with a size of less than 1 MB can become corrupted after granting access to more than 5 users or groups. (Bug was introduced in version 2.1.403.78)

Version 2.1.415.120 (2015-06-24)

- Fixed: Cannot rename on auto detected USB drives
- Fixed: In some cases adding a license to a local key file could corrupt the key file

Version 2.1.413.111 (2015-05-28)

- Fixed: Cannot eject removable drives when added as Boxcryptor location
- Fixed: Boxcryptor trying to add inaccessible network drives as location
- Fixed: Not showing complete directory if it contains an element with illegal characters
- Fixed: Cannot rename or move read-only files (e.g. in git repositories)
- Fixed: Leaving a group deleted the group instead
- Changed: Detected networked drives no longer get automatically enabled

Version 2.1.409.104 (2015-05-11)

- Added: Auto-detection for USB and network drives as Boxcryptor locations
- Fixed: Crash when Boxcryptor is started again while it is starting
- Fixed: Missing context menu on some special Windows setups
- Fixed: Add license with local account

Version 2.1.407.99 (2015-04-07)

- Fixed: Crash on startup when trying to start Boxcryptor two times
- Fixed: SMDiagnostics.dll causing Boxcryptor to crash
- Fixed: Error with drives as locations
- Fixed: Copying very large files to the Boxcryptor drive can fail under certain circumstances
- Improved: Write performance if an application expands the file before writing file contents. (E.g. Performance of copying files in Windows Explorer has been improved by 100%.)
- Improved: Better handling with multiple Windows users

Version 2.1.405.86 (2015-03-24)

- Improved: Display of encrypted icon overlay with high DPI displays and Windows scaling

Version 2.1.403.78 (2015-03-15)

- Added: Support for Telekom TeamDisk
- Added: Filename encryption can be enabled or disabled on existing folders. (Right-click -> Boxcryptor -> Enable/Disable filename encryption)
- Added: Filename encryption inheritance. New file or folders now inherit the filename encryption setting of their parent folder. If the name of the parent folder is encrypted (or not), the name of the new file or folder will also be encrypted (or not) - regardless of the filename encryption setting of the user.
- Improved: "Could not delete original folder" error message on encrypt / decrypt does not occur as often as before
- Fixed: "Out of memory" error message when encrypting large files
- Minor bug fixes and improvements

Version 2.1.401.69 (2015-02-26)

- Added: Auto-detection for Dropbox for Business and other providers with multiple sync folders
- Added: Auto-detection for new storage providers (e.g. OneDrive for Business, Strato HiDrive, iCloud Drive, CloudMe, Cubby, Web.de, TelekomCloud, Storegate, SpiderOak, and SafeSync)
- Added: Advanced option to turn off OneDrive online files info message
- Added: Installer is now also available in German

- Improved: Redesigned user interface
- Improved: Location handling for providers with a slow updating (e.g Webdav based provider)
- Improved: Encrypted files and folders are now highlighted with a green icon overlay with a lock instead of a green font
- Improved: Files and folders with encrypted names are now always shown in the Boxcryptor drive - regardless if they can be decrypted or not
- Fixed: "File has been externally altered" error
- Overall bug fixes and improvements

Version 2.0.437.408 (2014-10-27)

- Added: Support for Dropbox shared folders which are view-only
- Added: "Temporary file preservation" for encrypted files is now also applied to plaintext filenames - not only encrypted filenames. This improves temporary file detection by other applications, e.g. to exclude them from sync.
- Improved: OneDrive for Business auto-detection
- Minor bug fixes and improvements

Version 2.0.435.407 (2014-09-15)

- Improved: Handling of sync conflicts / conflicted copies.
- Minor bug fixes and improvements

Version 2.0.433.406 (2014-09-02)

- Fixed: Wrong file sizes in GoodSync on network shares.

Version 2.0.431.403 (2014-08-06)

- Improved: Better handling for sync conflicts / conflicted copies.
- Encrypted file names which have been modified (e.g. by appending " (conflicted copy)") are now auto-fixed by including the suffix automatically into the encrypted file name.
- The conflicted copy then also appears in the Boxcryptor Drive.
- Improved: Box Sync auto-detection.
- Fixed: Dragon Natural Speaking cannot load profile located on the Boxcryptor Drive.
- Fixed: SecureCRT cannot save log files on the Boxcryptor Drive.

Version 2.0.429.396 (2014-07-11)

- Fixed: Moving a plaintext file to an encrypted folder failed.
- Fixed: Some applications could not save a file in a location on a network share.

Version 2.0.427.395 (2014-06-30)

- Fixed: Folder is empty because one file contains invalid characters (e.g. '<' or '>' which are not allowed on Windows file systems). Such files are now skipped and ignored.
- Fixed: Boxcryptor Drive cannot be opened "Invalid parameter" in certain circumstances when a location is on a network share.

Version 2.0.425.394 (2014-06-23)

- Fixed: Box Sync 3 was not auto-detected.
- Fixed: "Save as" in Internet Explorer did not work anymore.

Version 2.0.423.392 (2014-06-16)

- Fixed: File was not saved correctly after being rotated in Windows Photo Viewer.
- Fixed: Cannot open Quicken file.

Version 2.0.421.388 (2014-06-11)

- Improved: File save in Microsoft Office (Word, Excel, etc.) and other applications which use temporary files
- Improved: Handling of reset accounts
- Fixed: Box does not sync permission changes

Version 2.0.419.376 (2014-04-10)

- Added: OneDrive for Business support

Version 2.0.417.367 (2014-02-24)

- Autoupdate activated!
- Fixed: File times are modified on permission change
- Fixed: Microsoft OneDrive is not auto-detected on Windows 7

Version 2.0.415.357 (2014-02-20)

- Fixed Box Sync 4.0 auto-detection
- Improved Permissions Management
- Better feedback for context-menu encrypt/decrypt
- Improved CBFS driver install
- Improved auto-update process

Version 2.0.413.343 (2013-12-19)

- Updated CBFS to v4.0.139
- Changed: Renamed "Share Access" to "Manage Permissions" to avoid misunderstandings with the word "Sharing" used by cloud storage providers.

Version 2.0.411.330 (2013-11-07)

- Fixed: Recycle bin doesn't work
- Fixed: Encrypt read-only files fails with path already exists
- Fixed: Modified date is set on read

Version 2.0.409.325 (2013-11-07)

- Added: Option to disable Volume Watcher notifications
- Fixed: Hide files beginning with . does not work
- Fixed: Logout from local account forgets to remember email address
- Fixed: Newly created group is not removed properly on deletion
- Fixed: Windows 8.1 search index does not work (Enable both options "Mount in Windows Mount Manager" and "Mount For all Users")
- Minor bug fixes and improvements

Version 2.0.407.311 (2013-10-15)

- Improved: Performance (especially when using network shares / WebDAV)
- Improved: Copying many files fails with „Externally altered“
- Fixed: SkyDrive in Windows 8.1 does not show any files
- Fixed: Cannot use “Remember password” with local account
- Fixed: Same IVs are used for all files/folders within one Boxcryptor session
- Fixed: Cannot remove a deleted user from sharing
- Fixed: Cannot create new files or folders in a folder shared with a deleted user
- Minor bug fixes and improvements
- (Change to 308: SkyDrive detection in Windows 8)

Version 2.0.405.295 (2013-09-24)

- Added: Ability to use custom keys using the command line argument /customkeys
- The custom key feature
- Added: Compatibility with Microsoft SyncToy
- Fixed: Enable locations after logout and login was not working
- Fixed: Boxcryptor crash if key file was not found in local mode
- Fixed: Cannot move a file when source and target are on different drives
- Fixed: Various smaller issues
- Fixed: Cannot create a stable subkey under a volatile parent key.

Version 2.0.403.275 (2013-08-26)

- Fixed: Pipe Error 5, when encrypting / decrypting.
- Changed: Contact Information.

Version 2.0.403.272 (2013-08-26)

- Changed: Fallback for opening pipe without elevated rights

Version 2.0.403.269 (2013-08-26)

- Fixed: Sharing violation when loading settings (cache.db)
- Fixed: Boxcryptor cannot be used with drives as location
- Fixed: Login is possible when currently logging in or mounting the drive
- Fixed: Collection modified by multiple threads when saving cache
- Fixed: ReadyBoost causes error message
- Fixed: Wrong error message when account locked
- Fixed: Open plaintext dialogs and exit leads to blocking windows explorer
- Fixed: Pipe-Error 5 if Boxcryptor runs as admin
- Fixed: Boxcryptor cannot be used with network shares as location
- Fixed: Outlook cannot attach an encrypted file when EFS is disabled
- Fixed: Prevent decryption when saving an encrypted file in a plaintext folder
- Added: Prevent copying of .bc files to drive
- Added: Show information about installing CBFS in installer
- Added: Setting for disabling the creation of the favorites link (Boxcryptor.exe.config "CreateFavoritesLink")
- Added: Support for alternative filemanagers (Altap Salamander, Cubic Explorer, Directory Opus, Explorer++, Far Manager, FreeComander, SpeedComander, Total Commander, TeraCopy, xplorer2, XYplorer)

Version 2.0.402.252 (2013-08-09)

- Added: Interactive Tour after sign up
- Added: When creating a file or folder in a plain text folder a dialog pops up asking the user if he wants to encrypt the file or folder (This dialog can be disabled by adding '"dontConfirmPlaintextOperation": true' in %LOCALAPPDATA%\Boxcryptor\volume.db)
- Added: Locations in the Boxcryptor Drive are updated on-the-fly without the need to refresh
- Fixed: Improved compatibility with MS Office
- Fixed: Files with plain text filenames are deleted on rename with capitalization change only
- Fixed: Plain text files or folders are not shown in the Boxcryptor Drive if they contained certain Asian UTF-8 characters
- Fixed: Locking the master key requires restart to take effect
- Fixed: Update check
- Fixed: Various smaller issues, bugs and UI improvements

Version 2.0.401.229 (2013-07-23)

- Fixed: Several fixes and improvements regarding the installer
- Added: Disable Encrypting File System (EFS) during installation
- Added: Support for default proxy servers
- Fixed: Encrypting of files with non-ascii characters failed
- Fixed: Boxcryptor start with Windows, even though the option was not checked
- Fixed: Master Key cannot be unlocked if a user in the company has expired keys

Version 2.0.401.172 (2013-06-28)

- Fixed: Installer not installing Callback FileSystem

Version 2.0.401.170 (2013-06-27)

- Fixed: Uninstaller crashing

Version 2.0.400.166 (2013-06-25)

- Added: Boxcryptor icon for folder keys
- Added: Confirmation before decrypting files
- Fixed: Progress while importing files
- Fixed: Cannot create files in shared folders
- Fixed: Minor fixes and improvements

Version 2.0.400.153 (2013-06-20)

- Added: A shortcut to the Boxcryptor Drive in the Windows Favorites section
- Added: Decrypt Option Added: Progress indication while encrypting / decrypting
- Added: Shortcut to change the path to the key file Fixed: Minor fixes and improvements

Version 2.0.400.146 (2013-06-17)

- Removed context-menu placeholder for "Decrypt"

Version 2.0.400.145 (2013-06-15)

- Added context-menu placeholder for "Decrypt"
- Fixed: Norton classifies Boxcryptor as suspicious due to missing dll signatures

Version 2.0.400.138 (2013-06-14)

- Changed: Increased default KDF iterations for new keys from 5.000 to 10.00
- Changed: Context-menu "Encrypt" does not use a temporary folder anymore
- Fixed: Context-menu does not work when Kaspersky AV is installed
- Fixed: Context-menu "Encrypt" fails if Preview Pane in Windows Explorer is activated
- Fixed: Directory Opus fails with invalid parameter to copy pdf file
- Fixed: Boxcryptor cannot be installed on removable drives
- Fixed: Minor fixes and improvments

Version 2.0.400.121 (2013-06-07)

- Updated CBFS to v4.0.135.22
- Fixed: Minor fixes and improvements

Version 2.0.400.116 (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