Einführung

Was ist die Cloud?

> Es gibt keine Cloud. Es gibt nur den Computer eines Anderen.

Mobile Geräte und Cloud-Speicher haben die Art und Weise, wie wir mit Dateien arbeiten, grundlegend verändert. Dateien müssen auf allen Geräten und für alle, die Zugang benötigen, **verfügbar** sein. Anbieter wie Dropbox, OneDrive oder Google Drive, erfüllen diese Vorraussetzung und kümmern sich für Sie um die Speicherung Ihrer Dateien. Sie speichern **Ihre Dateien auf deren Servern** und synchronisieren sie auf jedes verbundene Gerät.

Während die Cloud viele Vorteile bietet, wie automatische Backups oder eine Verringerung der Kosten für Hardware, bezahlen Sie mit **dem Verlust der Kontrolle über Ihre Daten**. Jeder, der Zugriff auf den Server des Cloud-Anbieters hat, kann Ihre Daten lesen.

Was ist Boxcryptor?

Boxcryptor bietet durch die **lokale Verschlüsselung** von Dateien auf dem Gerät eine zusätzliche und **benutzerfreundliche** Sicherheitsschicht für Cloud-Speicher. Da Boxcryptor von Anfang an **für die Cloud optimiert** wurde, erfolgt die Verschlüsselung **dateibasiert** und der Zugriff auf verschlüsselte Dateien kann geteilt werden. Das bedeutet, dass jede Datei **unabhängig** von den anderen Dateien verschlüsselt wird.

Was Boxcryptor **nicht** ist

- Boxcryptor ist **kein Cloud-Speicheranbieter**. Es ist eine Sicherheitssoftware die eine zusätzliche Sicherheitsschicht zum Cloud-Speicher Ihrer Wahl hinzufügt. Boxcryptor speichert Ihre Dateien somit nicht selbst. Die Verantwortung für die Speicherung und Verwaltung Ihrer Dateien liegt beim Cloud-Speicheranbieter.

- Auf **Windows** ist Boxcryptor ist **kein Synchronisationsdienst**. Das bedeutet, dass Boxcryptor hier **keine** Dateien in die Cloud synchronisiert. Die Verantwortung für die Speicherung und Verwaltung Ihrer Dateien liegt beim Cloud-Speicheranbieter. Um Dateien zu synchronisieren muss die Software Ihres Cloud-Speicherdienstes installiert werden.
- Boxcryptor wurde **nicht für beliebige Cloud-Dienste** entwickelt. Dienste wie Google Docs oder Evernote arbeiten nicht mit lokalen Dateien sondern speichern die Daten direkt auf ihren Servern. Boxcryptor kann nur Dateien verschlüsseln, die lokal gespeichert werden.
- Boxcryptor ist **keine VPN-Lösung**. Obwohl wir Partnerschaften mit verschiedenen VPN-Anbietern haben, sind wir technisch in keiner Weise mit deren Produkten verbunden.

Quickstart

Sind Sie bereit, Ihre Cloud-Speicher abzusichern? Diese Anleitung hilft Ihnen bei den ersten Schritten mit Boxcryptor und Ihrer Cloud.

Boxcryptor installieren

Um Boxcryptor auf Ihrem Mac zu installieren, laden Sie sich die gewünschte Version von unserer Website herunter.

> Wenn Sie Boxcryptor das erste Mal starten, werden Sie aufgefordert, die Installation durch Eingabe der Anmeldedaten Ihres **macOS-Kontos** (mit Adminrechten) abzuschließen. Das sind **nicht** Ihre Anmeldedaten für Boxcryptor.

Installationshinweise für Boxcryptor (3.x)

Benötigte macOS Version:

- Benötigt **macOS 12.0** oder später. Bitte beachten Sie, dass wir offiziell keine Betaversionen von macOS unterstützen. Neue macOS-Versionen werden jedoch von Boxcryptor unterstützt, sobald sie offiziell von Apple veröffentlicht werden – manchmal sogar etwas früher.

Datei Synchronisation:

- Boxcryptor 3.x **beinhaltet die volle Funktionalität für eine schnelle, reibungslose und sichere Synchronisierung Ihrer Dateien und Ordner.** Es ist alles, was Sie auf Ihrem Mac installieren müssen, um mit verschlüsselten Dateien in Dropbox, OneDrive, Google Drive oder jedem anderen unterstützten Cloud-Anbieter zu arbeiten. Sie können den Client Ihres Cloud-Anbieters von Ihrem Mac entfernen.

Sicherheit:

- Boxcryptor 3.x ist eine native "File Provider"-App, die auf modernen macOS-Betriebssystemen "out-of-the-box" funktioniert. Außerdem nutzt die App den macOS-Sandboxing-Sicherheitsmechanismus vollständig aus.

Verschlüsselung lokal gespeicherter Dateien:

- Dateien, die lokal auf Ihrem Mac gespeichert sind, werden von Boxcryptor nicht mehr verschlüsselt, da Apples File-Provider-Plattform technische Beschränkungen auferlegt. File-Provider-Apps müssen Dateien im Klartext im lokalen Dateisystem speichern, damit ihr Inhalt von macOS erfasst und dem Benutzer angezeigt werden kann. Dies betrifft Dateiinhalte und Dateinamen.
- Hier ist der Verschlüsselungsstatus nach Standort:
  - **In der Cloud:** Dateien sind immer durch die Verschlüsselung von Boxcryptor geschützt.

    - **Auf Ihrem Mac mit FileVault:** Dateien werden durch die Verschlüsselung von FileVault geschützt.
    - **Auf Ihrem Mac ohne FileVault:** Dateien sind nicht geschützt (nicht empfohlen)
- **Wir empfehlen dringend die Verwendung einer lokalen Festplattenverschlüsselung für jeden Mac** - unabhängig davon, ob Sie eine frühere Version von Boxcryptor für macOS oder die neue Boxcryptor für macOS Beta verwenden oder sogar, wenn Sie Boxcryptor überhaupt nicht verwenden. Die Festplattenverschlüsselung ist ein integraler Bestandteil der Sicherheit lokaler Geräte und kann leicht umgesetzt werden werden, indem FileVault auf jedem Mac aktiviert wird.

> Durch die Verwendung von **FileVault** sind Dateien, die im neuen Boxcryptor für macOS Beta verfügbar sind, immer noch durch die Verschlüsselung von FileVault auf der lokalen Festplatte geschützt, obwohl sie als Klartext erscheinen, wenn Ihr Mac in Gebrauch ist. Erfahren Sie hier mehr über FileVault: https://support.apple.com/en-us/HT204837

Spotlight:

- Ein großer Vorteil der File Provider-API ist, dass Spotlight sofort funktioniert, ohne dass Boxcryptor etwas besonders behandeln muss. Das bedeutet, dass **Spotlight besuchte Dateien und Ordner in Boxcryptor-Speicherorten automatisch und standardmäßig indiziert.** Die Spotlight-Unterstützung ist keine optionale erweiterte Einstellung mehr, sondern ein erstklassiges Standard-Erlebnis für jeden Benutzer.

Installationshinweise für (legacy) Boxcryptor 2.x

Benötigte macOS Version:

- Benötigt **macOS 10.15** oder später.

Datei Synchronisation:

- Boxcryptor erfordert, dass der Sync-Client Ihres Cloud-Anbieters auf Ihrem System installiert ist. Die meisten Clouds werden von Boxcryptor automatisch erkannt und als Speicherort zum Boxcryptor-Laufwerk hinzugefügt. Wenn Ihre Cloud nicht automatisch erkannt wird, können Sie sie manuell als benutzerdefinierten Speicherort hinzufügen.

Sicherheit:

- Aufgrund der Strategie von Apple, Kernel-Erweiterungen von Drittanbietern in macOS zu verbieten, um das Mac-Betriebssystem weiter abzusichern und abzuschotten, hat das Unternehmen vor einigen Jahren damit begonnen, Kernel-Erweiterungen von Drittanbietern nicht länger zu unterstützen und ihre Verwendung sukzessive zu erschweren. Während in der Vergangenheit eine Kernel-Erweiterung "on-the-fly" geladen werden konnte, erfordert macOS 10.15 Catalina nun einen Neustart des Systems während des Ladevorgangs. Macs mit Apple-Silicon-Prozessoren benötigen zusätzlich die Änderung der Sicherheitsrichtlinien des Macs im Recovery Mode, um das Laden von Kernel-Erweiterungen von Drittanbietern zu ermöglichen.

Erforderliche Systemerweiterung

Boxcryptor v2 enthält eine Systemerweiterung, die für die Bereitstellung des Boxcryptor-Laufwerks benötigt wird. Systemerweiterungen werden in macOS 10.13 und neuer standardmäßig blockiert so dass Sie beim ersten Start **das Laden von Systemsoftware des Entwicklers "Benjamin Fleischer" erlauben** müssen. Benjamin ist der Maintainer der von Boxcryptor verwendeten Open Source Systemerweiterung.

Verschlüsselung lokal gespeicherter Dateien:

- Boxcryptor v2 verschlüsselt alle lokal gespeicherten Dateien.

Spotlight:

- Nicht länger unterstützt.

Ein Boxcryptor-Konto erstellen

⚠ Mit dem Anschluss Boxcryptors an Dropbox können keine neuen Boxcryptor-Konten erstellt werden.

Unser Ziel ist es, Ihnen die Verwaltung Ihrer verschlüsselten Dateien so einfach wie möglich zu machen.

1. Starten Sie **Boxcryptor**.
2. Klicken Sie auf **Konto erstellen**.
3. Folgen Sie den Anweisungen des Assistenten.

Wählen Sie ein Passwort, das Sie sich merken können oder bewahren Sie das Passwort an einem sicheren Ort auf, wie zum Beispiel einem Passwortmanager. Boxcryptor folgt dem Zero-Knowledge-Prinzip, daher können wir Ihr Passwort **nicht** zurücksetzen.

ⓘ Wenn Sie Ihr Passwort vergessen, sind Ihre Daten irreversibel verloren.

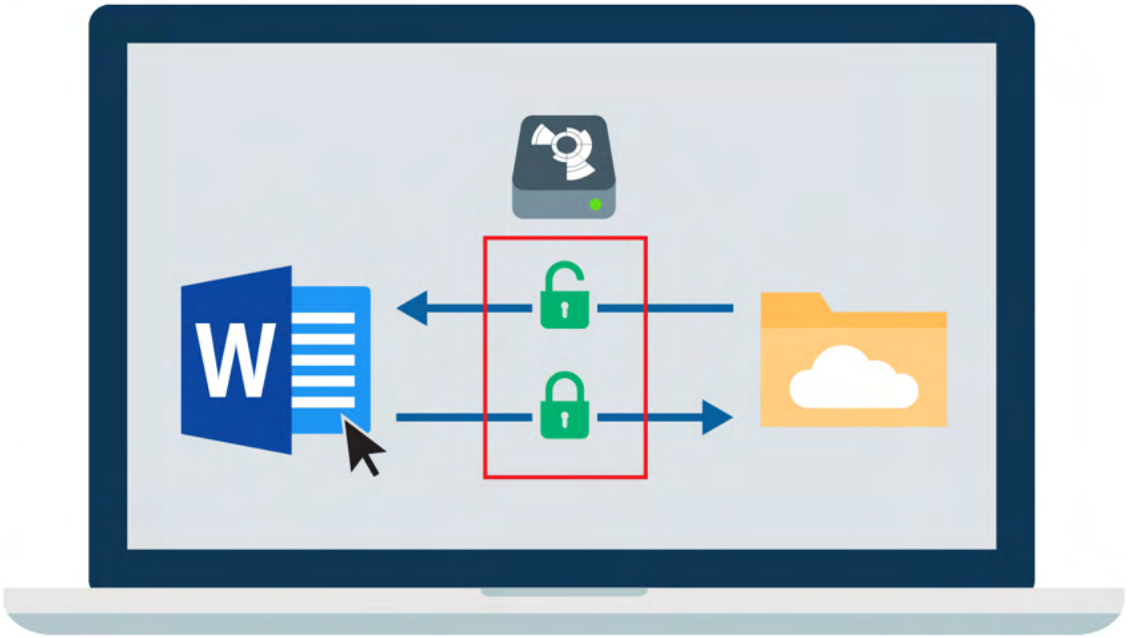
ⓘ Aufgrund von Einschränkungen von Apple ist es nicht möglich, ein Boxcryptor-Konto innerhalb der macOS-App zu erstellen. Bevor Sie Boxcryptor für macOS verwenden, müssen Sie zuerst auf unserer Webseite Ihr Konto erstellen.

Entdecken Sie Boxcryptor

Nachdem Sie Boxcryptor installiert und sich mit Ihrem Boxcryptor-Konto angemeldet haben,

können Sie Ihren Cloud-Anbieter hinzufügen und auf Ihre Dateien zugreifen.

Ab jetzt können Sie Boxcryptor benutzen, um mit Ihren Dateien in der Cloud zu arbeiten. Die App verbindet sich direkt mit Ihrem Cloud-Anbieter und kümmert sich um das Hoch- und Herunterladen Ihrer Dateien, sowie um die Entschlüsselung.



Kleine Symbole markieren Dateien und zeigen Ihnen, ob eine Datei oder ein Ordner verschlüsselt ist oder nicht.

Sie können die Boxcryptor-App öffnen, indem Sie auf das Boxcryptor-Symbol in der Menüleiste klicken. Um die Speicherort Ihrer Cloud-Anbieter zu durchsuchen, klicken Sie entweder hier auf den gewünschten Speicherort oder öffnen Sie den Finder und gehen Sie zum Abschnitt **Orte** in der Seitenleiste.

Ihr erster verschlüsselter Ordner

Alle Dateien und Ordner, die Sie in Boxcryptor hinzufügen, werden **automatisch verschlüsselt**. So gehen Sie vor, wenn Sie Boxcryptor das erste Mal verwenden und noch keine Dateien in Ihrer Cloud haben.

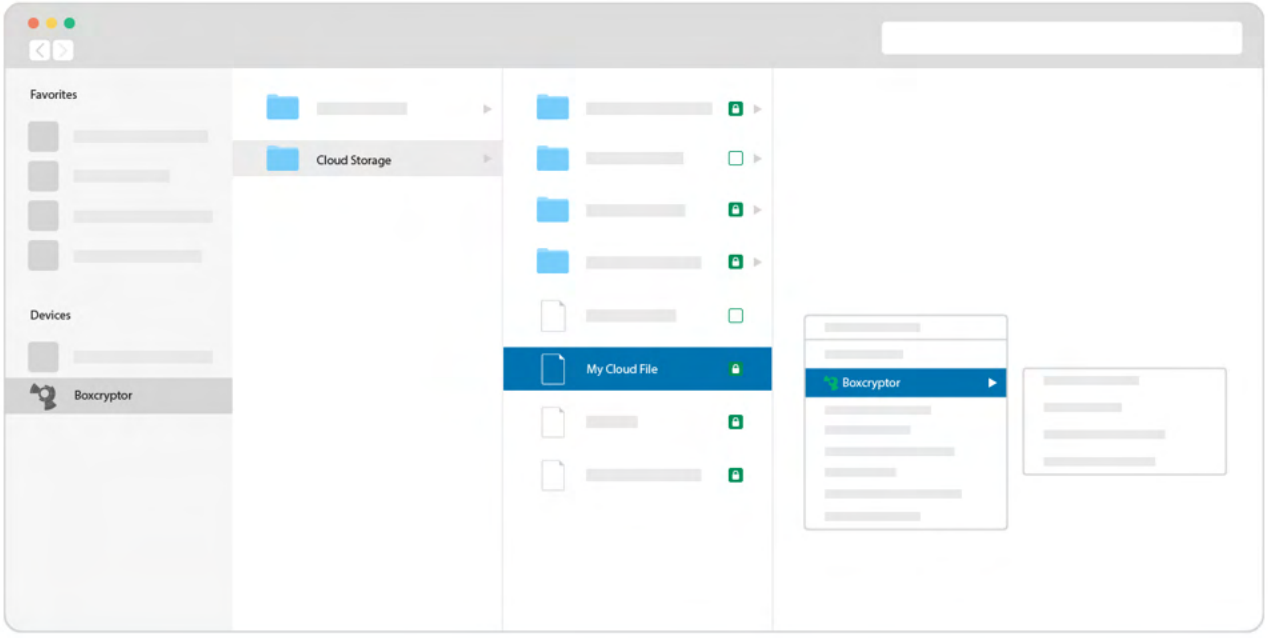
1. Öffnen Sie den **Boxcryptor-Ort** Ihres gewünschten Cloud-Speicher Anbieters.
2. Klick auf ⋯ → **Neuer Ordner**.
3. Fügen Sie dem Ordner Dateien hinzu. Alle Dateien werden automatisch verschlüsselt und erben auch alle eingestellten Boxcryptor Berechtigungen.

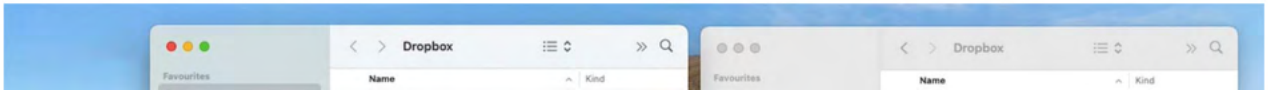
Wie man bestehende Dateien verschlüsselt

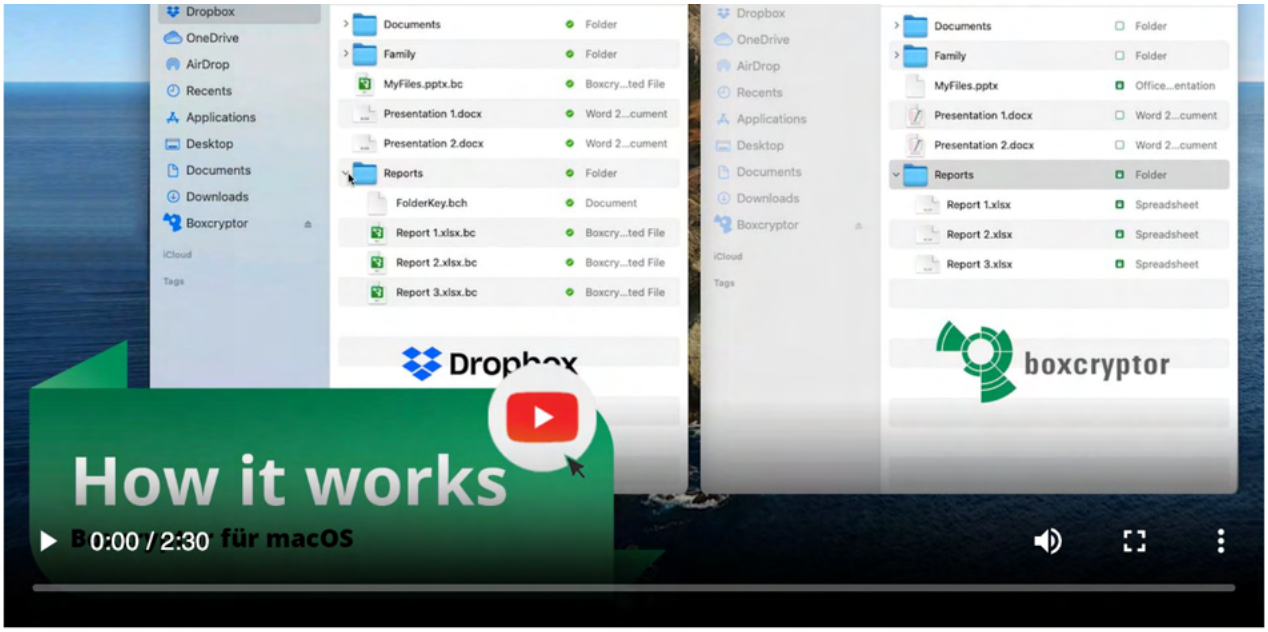
Wenn Sie bereits Dateien oder Ordner in Ihrer Cloud gespeichert haben, kann Boxcryptor diese ebenfalls verschlüsseln.

1. Wählen Sie Ihren **Boxcryptor-Ort**.
2. **ctrl-Klick** auf eine Datei oder einen Ordner → **Verschlüsselte Kopie erstellen**.
3. Wählen sie die gewünschten Zugriffsberechtigungen aus und bestätigen Sie anschließend die Operation.

Boxcryptor wird nun eine verschlüsselte Kopie der Auswahl erstellen und sie automatisch bei Ihrem Cloud-Anbieter hochladen.






Dropbox
OneDrive
AirDrop
Recents
Applications
Desktop
Documents
Downloads
Boxcryptor
iCloud
Tags
Documents Folder
Family Folder
MyFiles.pptx.bc Boxcry...ted File
Presentation 1.docx Word 2...cument
Presentation 2.docx Word 2...cument
Reports Folder
FolderKey.bch Document
Report 1.xlsx.bc Boxcry...ted File
Report 2.xlsx.bc Boxcry...ted File
Report 3.xlsx.bc Boxcry...ted File
MyFiles.pptx Office...entation
Report 1.xlsx Spreadsheet
Report 2.xlsx Spreadsheet
Report 3.xlsx Spreadsheet
boxcryptor
How it works
0:00 / 2:30

Verwalten Sie Ihre Clouds und Speicherorte

Boxcryptor unterstützt standardmäßig eine Vielzahl von Cloud-Speicheranbietern. Darüber hinaus funktioniert Boxcryptor mit jedem Cloud-Anbieter, der das WebDAV-Protokoll unterstützt.

Speicherort hinzufügen

Boxcryptor ist eine **zusätzliche Sicherheitsebene** für Ihren Cloud-Speicher. Auf macOS **verbinden wir uns direkt** mit Ihrem Anbieter und kümmern uns sowohl um das Hochladen, als auch um die Verschlüsselung Ihrer Dateien. Um einen neuen Anbieter zu Boxcryptor hinzuzufügen, folgen Sie bitte diesen Schritten:

1. Öffnen Sie die **Boxcryptor App** und navigieren Sie zu **Start**.
2. Klicken Sie auf **Anbieter hinzufügen** und wählen Sie ihren Cloud-Anbieter aus.
3. Erlauben Sie Boxcryptor sich bei ihrem Anbieter anzumelden und schließen Sie die Anmeldung ab.

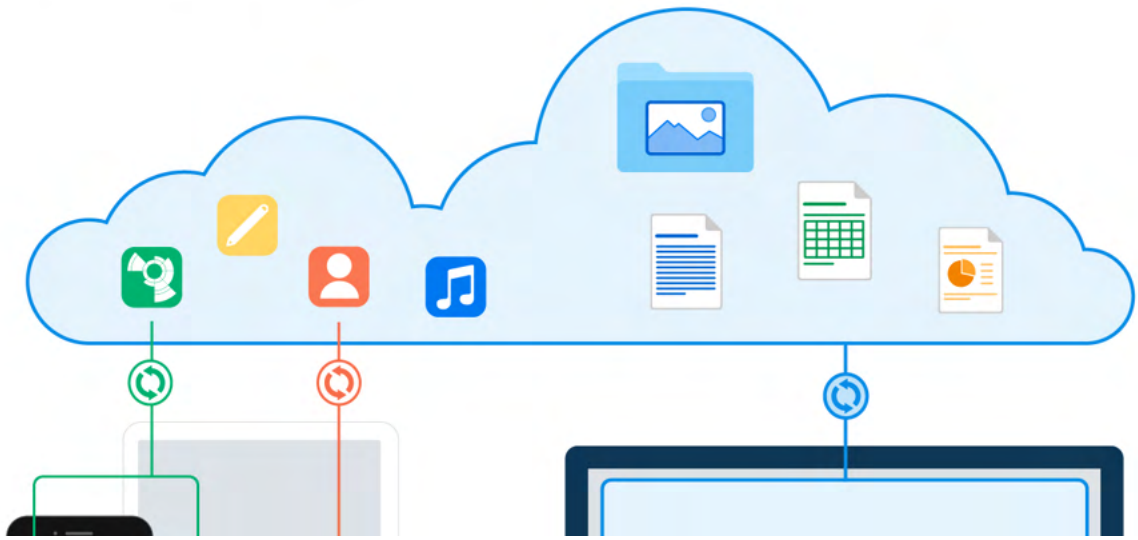
Sie können Ihren Provider auch durch ctrl-Klick **umbenennen** oder **löschen**.

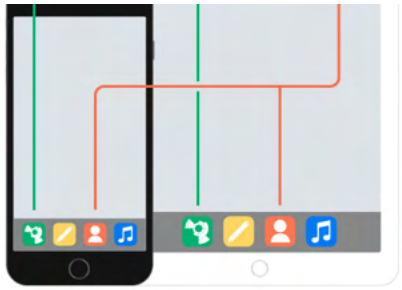
Google Drive

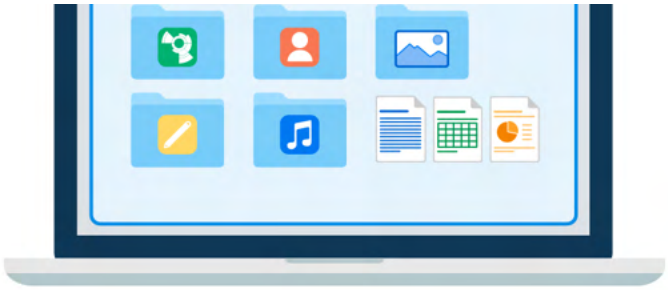
Boxcryptor ermöglicht den Zugriff auf Dateien in Google Drive's **Meine Ablage**, **Geteilte Ablagen** und **Freigegeben**. Zusätzliche gesicherte Ordner über **Mein Computer** sind *nicht* verfügbar.

iCloud

Aufgrund von technischen Einschränkungen von Apple, unterscheidet Boxcryptor für macOS zwischen **iCloud** und **iCloud Drive (nur Mac & PC)**. Wenn Sie vorhaben, Boxcryptor auf dem iPhone oder iPad zu benutzen, dann stellen Sie sicher, dass Sie **iCloud** nutzen, weil iCloud Drive nur auf dem Mac oder PC zur Verfügung steht.







Stellen Sie sicher, dass Sie dieselbe Apple ID auf Ihrem iOS-Gerät und Ihrem Mac benutzen.

Benutzerdefinierte Speicherorte

Boxcryptor unterstützt das Hinzufügen von Ordnern Ihres lokalen Dateisystem als **Lokaler Speicher**:

1. Öffnen Sie die **Boxcryptor App** und navigieren Sie zu **Start**.
2. Klicken Sie auf **Anbieter hinzufügen** und wählen Sie Ihren Cloud-Anbieter aus.
3. Klicken Sie auf **Lokaler Speicher** und wählen Sie Ihren eigenen, benutzerdefinierten Speicherort aus.

Falls Ihr gewählter Speicherort kein Ordner ist, der von einem Cloud-Anbieter synchronisiert wird, wird nichts in die Cloud hochgeladen. Die Daten bleiben lokal auf Ihrem Mac, wie jeder andere Ordner, aber verschlüsselt.

WebDAV-Speicherorte

Wenn Sie Ihren bevorzugten Cloud-Anbieter nicht in der Liste der unterstützten Anbieter finden, stehen die Chancen gut, dass Boxcryptor ihn trotzdem unterstützt. Viele Cloud-Anbieter benutzen das **WebDAV-Protokoll**, welches auch von Boxcryptor implementiert ist.

1. Fragen Sie Ihren Anbieter nach den WebDAV-Zugangsdaten.

Boxcryptor erfodert eine gesicherte Server-Verbindung (`https://`) mit einem gültigen bzw. auf dem Gerät installiertem selbst-signiertem SSL Zertifikat.

In lokalen Netzwerken sind zusätzlich IP-basierte unverschlüsselte Verbindungen (`http://`) möglich, sofern Sie das auf Ihrem Gerät zulassen.

2. Öffnen Sie die **Boxcryptor-App** und gehen Sie zu **Start**
3. Tippen Sie auf **Anbieter hinzufügen** und wählen Sie **WebDAV** aus.
4. Schließen Sie die Anmeldung mit den gegebenen WebDAV-Zugangsdaten ab.

ownCloud und **nextCloud** unterstützen WebDAV. Standardmäßig lauten die Konfigurations-URLs:
`https://example.com/owncloud/remote.php/webdav`

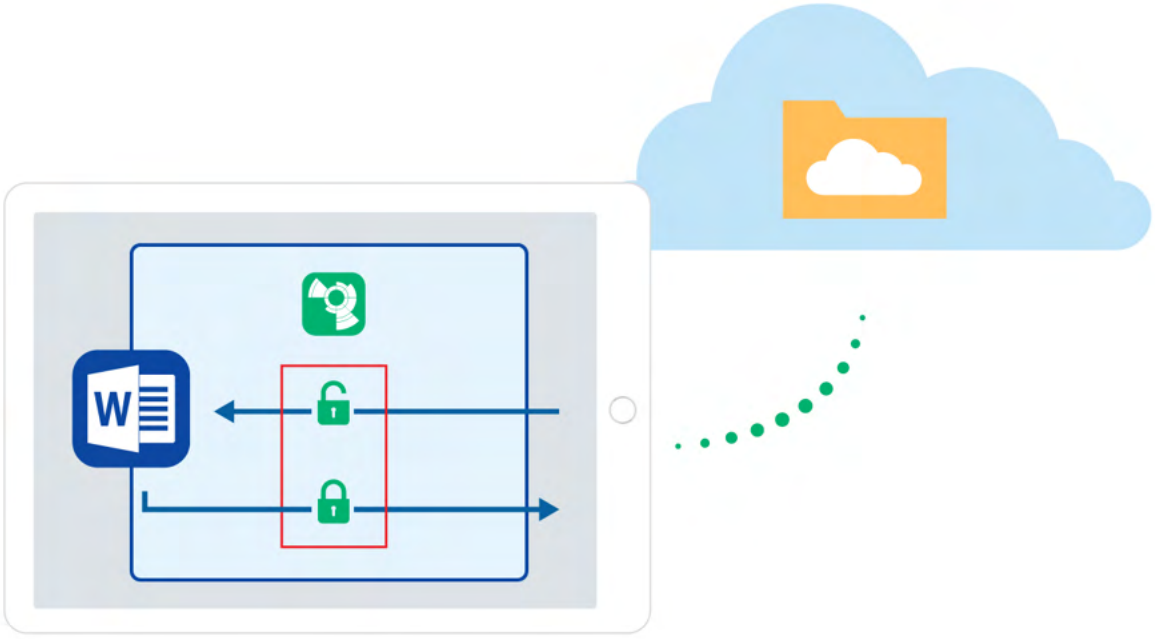
```
https://example.com/nextcloud/remote.php/dav/files/username/
```

Mit Dateien arbeiten

Unser Fokus liegt darauf, Boxcryptor so **benutzerfreundlich und einfach** wie möglich zu halten. Sobald Boxcryptor installiert ist, werden Sie nicht bemerken, dass Ihre Dateien verschlüsselt sind. Arbeiten Sie einfach in gewohnter Weise weiter.

On-the-Fly-Verschlüsselung

Boxcryptor verschlüsselt Ihre Daten **einzeln** und **direkt beim Hinzufügen**. Bei der Arbeit mit Ihren Dateien müssen Sie diese nicht manuell entschlüsseln. Wird eine verschlüsselte Datei geöffnet, wird deren Inhalt automatisch im Hintergrund entschlüsselt. Wenn Sie die Datei nach dem Bearbeiten speichern wollen, verschlüsselt Boxcryptor diese wieder automatisch. Das macht die Arbeit mit Ihren verschlüsselten Daten ganz einfach – ohne dass Sie irgendetwas von den kryptografischen Prozessen im Hintergrund mitbekommen.



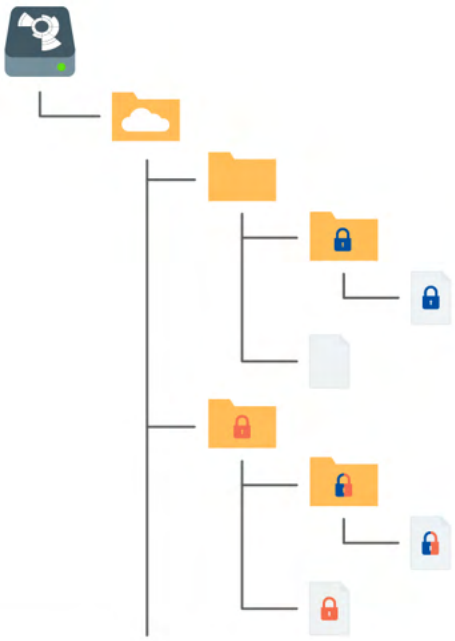
Wir entschlüsseln und verschlüsseln Ihre Dateien On-Demand: Sie wollen Ihre Inhalte sehen? Klicken Sie nur darauf und wir laden Ihre Datei für Sie herunter und entschlüsseln diese. Haben Sie Ihren Essay fertiggestellt? Speichern Sie es einfach in Boxcryptor und wir verschlüsseln die Datei und speichern sie in der Cloud.

Verschlüsselungs- und Berechtigungshierarchie

Sie können für jede Datei oder jedes Verzeichnis entscheiden, welches Sicherheits-Level Sie möchten. Boxcryptor gibt Ihnen darüber **volle Kontrolle**. Sie können anderen Personen erlauben auf eine Datei zuzugreifen, indem Sie diese berechtigen. Sie können ebenso wählen, ob der Dateiname verschlüsselt sein soll, oder Sie können einzelne Dateien und Verzeichnisse unverschlüsselt belassen.

Zur Vereinfachung **werden alle Eigenschaften einer Datei hierarchisch vom übergeordneten Verzeichnis geerbt**. Wenn Sie beispielsweise ein verschlüsseltes Verzeichnis mit Namen *My Secret Files* haben und Sie hier eine Datei hinzufügen, wird die Datei automatisch verschlüsselt und die

gewählten Berechtigungen werden geerbt. Das Gleiche trifft auf ganze Verzeichnisse zu.



Verschlüsselt und **Zugriffsberechtigung** für **Alice**

Verschlüsselt und **Zugriffsberechtigung** für **Bob**

Verschlüsselt und **Zugriffsberechtigung** für **Alice und Bob**

Anmerkung: Falls Sie eine Datei oder ein Verzeichnis ohne Verschlüsselung hinzufügen, wird Boxcryptor das Objekt automatisch verschlüsseln.

Mit Ihren Dateien arbeiten

Mit Boxcryptor müssen Sie **Dateien nicht manuell entschlüsseln** um damit zu arbeiten. Boxcryptor ist tief in macOS integriert und kann direkt im **Finder** unter **Orte** gefunden werden. Die Verschlüsselung findet on-the-fly statt. Deshalb werden alle anderen Programme, inklusive des Finders, **genauso funktionieren wie mit Dateien auf Ihrer Festplatte**.

Um mit Ihren verschlüsselten Dateien zu arbeiten, öffnen Sie den Boxcryptor-Ort im **Finder** und bearbeiten, betrachten, kopieren oder verschieben Sie Dateien wie in jedem anderen Ordner.

Falls Ihnen in Boxcryptor die Berechtigung fehlt, eine Datei zu öffnen, werden manche Programme Fehler anzeigen wie "kann nicht geöffnet werden" oder "Fehler -36"/"Error code -36". Stellen Sie In einem solchen Fall sicher, dass Sie die Berechtigung haben, die Datei zu öffnen. Dazu ctrl-klicken Sie auf **die Datei oder den Ordner** → **Berechtigungen verwalten**. Siehe auch Teilen mit Boxcryptor-Nutzern für weitere Informationen.

Wie Sie verschlüsselte Dateien erkennen

Boxcryptor ermöglicht es Ihnen, **verschlüsselte und unverschlüsselte** Dateien und Ordner im gleichen Verzeichnis zu verwalten. Verschlüsselte Dateien oder Ordner in Boxcryptor sind **mit einem kleinen Symbol markiert**.

verschlüsselt

Verschlüsselung vorhandener Dateien und Ordner

Wenn Sie bereits Dateien bei Ihrem Dienst gespeichert haben, können Sie Ihre bestehenden Dateien ebenfalls verschlüsseln. So funktionert es:

- Navigieren Sie zu der zu verschlüsselnden Datei oder dem zu verschlüsselnden Ordner.
- Ctrl-Klicken Sie die Auswahl und wähen Sie **Verschlüsselte Kopie erstellen** im Kontextmenü.
- Warten Sie die erfolgreiche Synchronisation ab.

Mit Dateinamenverschlüsselung arbeiten

Dateinamenverschlüsselung **verhindert wirksam die Analyse Ihrer Datenstrukturen durch Außenstehende**. Jedoch hat dies einen gewissen Einfluss auf die Geschwindigkeit der Anwendung und führt zu einem erhöhten Aufwand bei der richtigen Konfiguration. Sollten Sie Dateinamenverschlüsselung für geteilte Dateien und Verzeichnisse verwenden wollen, lesen Sie bitte unseren Blog-Post, speziell **Kapitel 5**, bevor Sie fortfahren.

> Eine mit Dateinamenverschlüsselung versehene Datei sieht so aus: 怕惊捋抱砻挤殥栟瞻擱斀漢怏搬濂檬溮楻捷抪柜欀賧.bc

Dateinamenverschlüsselung kann **global aktiviert** werden. Alle neu verschlüsselten Elemente, die nicht die Verschlüsselungs-Einstellungen ihres übergeordneten Verzeichnisses erben, werden mit Dateinamenverschlüsselung verschlüsselt. Existierende, verschlüsselte Dateien werden jedoch nicht angefasst. Das bedeutet, dass Sie bei existierenden Dateien die Dateinamenverschlüsselung manuell einschalten müssen.

Dateinamenverschlüsselung ist eine der Eigenschaften, die **Dateien von ihrem übergeordneten Verzeichnis erben**. Darum wird eine Datei, die in einem Verzeichnis mit Dateinamenverschlüsselung gespeichert wird, ebenfalls Dateinamenverschlüsselung haben.

> Selbst wenn die Dateinamenverschlüsselung global aktiviert ist, weisen neue Dateien, die in einem Ordner *ohne* Dateinamenverschlüsselung erstellt werden, aufgrund der Vererbung der Verschlüsselungseigenschaften *keine* Dateinamenverschlüsselung auf.

Um die Dateinamenverschlüsselung global zu aktivieren, gehen Sie zu **Einstellungen** und wählen Sie **Dateinamenverschlüsselung aktivieren**.

Um die Dateinamenverschlüsselungs-Einstellungen von bereits verschlüsselten Dateien und Ordnern zu verändern, führen Sie einen ctrl-Klick auf sie aus und wählen Sie **Dateiname verschlüsseln** im Kontextmenü.

Wie Dateien entschlüsselt werden

Sie müssen Ihre Dateien **nicht** entschlüsseln, wenn Sie mit Boxcryptor arbeiten.

So können Sie Dateien dennoch entschlüsseln, wenn dies erforderlich sein sollte:

- Wenn Sie möchten, dass die Dateien unverschlüsselt mit Ihrem Cloud-Anbieter synchronisiert werden: Ctrl-Klicken Sie auf die Datei oder den Ordner, den Sie entschlüsseln möchten, und wählen Sie **Entschlüsselte Kopie erstellen** .
- Wenn Sie Ihre Dateien im entschlüsselten Modus kopieren oder verschieben möchten: Wählen Sie einfach die Dateien im Boxcryptor-Ort im Finder aus und kopieren Sie diese an den neuen Speicherort. Die Daten werden automatisch entschlüsselt.

On-Demand-Dateien

Der Finder hat eine eingebaute On-Demand-Dateien-Funktion, was bedeutet, dass nicht alle Dateien automatisch mit Ihrem Gerät synchronisiert werden. Stattdessen wird nur die Verzeichnisstruktur auf Ihrem Gerät repliziert und die Dateien werden on-Demand heruntergeladen, wenn Sie sie öffnen oder herunterladen (**Ctrl-Klick -> "Jetzt herunterladen"**). Dies spart wertvollen Speicherplatz und Bandbreite, während Sie trotzdem auf jede Datei von Ihrem Computer aus zugreifen können. Wenn Sie später entscheiden, dass Sie die Datei lokal nicht mehr benötigen, können Sie sie einfach mit **Ctrl-Klick -> "Download entfernen"** entfernen. Wenn Sie in einen Ordner hinein navigieren, werden alle heruntergeladenen Dateien synchronisiert.

Zugriff auf Dateien teilen

Einer der Gründe für die Cloud ist das einfache Teilen von Dateien und die Möglichkeit der einfachen Zusammenarbeit. Boxcryptor ermöglicht es Ihnen dies auf eine sichere Art und Weise.

Was Sie über das Teilen von verschlüsselten Dateien wissen müssen

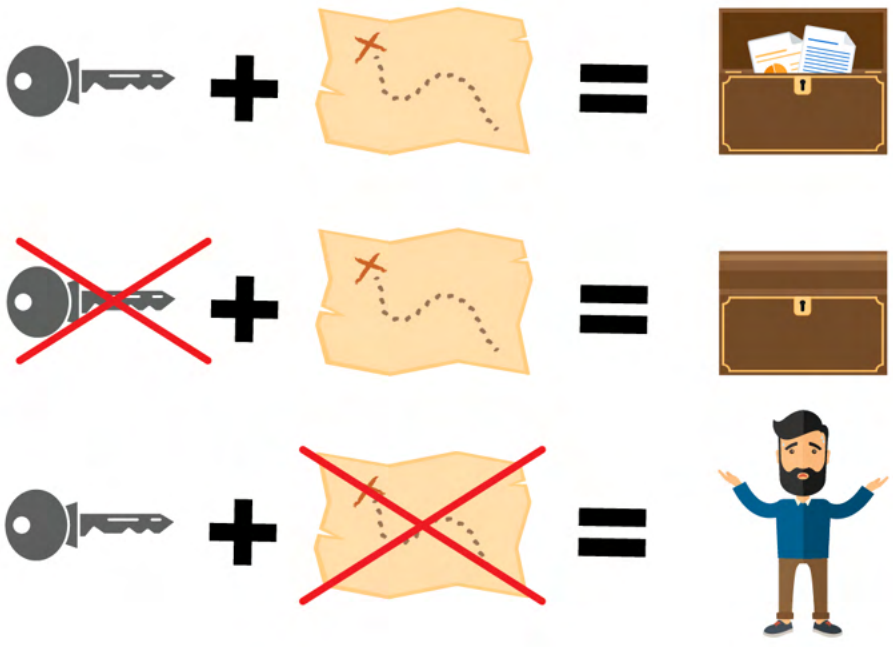
Um zu verstehen, wie das Teilen von verschlüsselten Datein funktioniert, ist es hilfreich zu wissen, wie Programme unverschlüsselte und verschlüsselte Datein behandeln.

Wenn Sie eine unverschlüsselte Datei auf Ihrem Gerät oder in der Cloud speichern, speichert das von Ihnen gewählte Programm die Datei und die darin enthaltenen Informationen. Diese Datei kann dann von jedermann, der physischen Zugang hat, gelesen oder verändert werden. Wenn Sie eine Datei jedoch verschlüsseln, werden die Informationen in der Datei modizifiert. Für Programme und Nutzer werden die verschlüsselten Informationen somit nutzlos. Um die Informationen wieder zu entschlüsseln, benötigen Sie einen **kryptographischen Schlüssel**, der die Informationen in den Originalzustand zurücksetzt.

Wenn Sie **eine verschlüsselte Datei teilen** ist das daher ungefähr so als ob Sie eine verworren getippte E-Mail verschicken. Die andere Person kann die Informationen zwar lesen, aber sie ist nutzlos, da **die semantische Bedeutung vollkommen fehlt**.

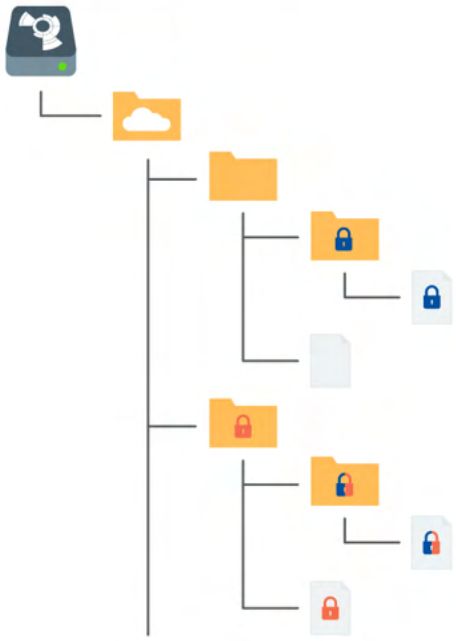
Deshalb sind zwei Schritte nötig, um eine verschlüsselte Datei zu teilen:

1. Teilen Sie die Datei physisch bei Ihrem Cloud-Anbieter. Bitte lesen Sie in der Dokumentation Ihres Anbieters nach, wie Dateien oder Verzeichnisse geteilt werden können.
2. Teilen Sie den kryptographischen Schlüssel in Boxcryptor. Boxcryptor verwendet für jede Datei einen Schlüssel. Der Schlüssel wird in Ihrem Boxcryptor-Konto verschlüsselt und **direkt in der Datei** gespeichert. Wenn Sie die Datei mit jemandem teilen, wird der Schlüssel mit dem Boxcryptor-Konto des Empfängers verschlüsselt und ebenso in der Datei gespeichert.



Hinweis: Jedesmal wenn Sie eine Datei teilen, wird diese modifiziert. Denken Sie daran, dass die Datei mit Ihrem Cloud-Anbieter synchronisiert werden muss. Wenn Sie den Zugang zu mehreren Dateien teilen, stellen Sie sicher, dass alle Dateien komplett synchronisiert werden.

So wie die Verschlüsselungseigenschaften vererbt werden, werden auch die Zugriffsrechte vom Hauptverzeichnis aus vererbt. Wenn Sie in einem geteilten Verzeichnis eine Datei hinzufügen, haben alle Personen, mit denen Sie das Verzeichnis teilen, Zugang zu dieser Datei.



verschlüsselt und **Zugriffsberechtigung** für **Alice**

verschlüsselt und **Zugriffsberechtigung** für **Bob**

verschlüsselt und **Zugriffsberechtigung** für **Alice und Bob**

Dateien mit Boxcryptor-Nutzern teilen: Berechtigungen

Wenn Sie eine Datei oder einen Ordner mit jemandem teilen möchten, der ebenfalls Boxcryptor verwendet, führen Sie die folgenden Schritte aus:

- Ctrl-Klick auf **Datei oder Ordner** → **Berechtigungen verwalten**.
- Fügen Sie die Gruppe oder den Nutzer hinzu, mit dem Sie die Datei oder den Ordner teilen möchten.
- Speichern Sie die Änderungen.
- Warten Sie, bis die Änderungen in die Cloud synchronisiert wurden.
- Stellen Sie sicher, zusätzlich den Zugriff auf die Datei oder den Ordner über das **Web-Interface Ihres Anbieters** zu teilen.

Falls Sie die Dateinamenverschlüsselung aktiviert haben, ist die beste Vorgehensweise, einen übergeordneten Ordner ohne Dateinamenverschlüsselung zu erzeugen und diesen Ordner über Ihren Cloud-Anbieter zu teilen.

Dateien mit Personen teilen, die Boxcryptor nicht nutzen:

Whisply

Wenn Sie eine Datei mit jemandem teilen möchten, der weder Boxcryptor noch eine Cloud nutzt, können Sie Whisply verwenden. Whisply ist ein Browser-basierter, sicherer Dateitransferdienst, den wir zu diesem Zweck entwickelt haben. Bitte folgen Sie der Boxcryptor und Whisply Anleitung hier.

Gruppen verwalten

Gruppen sind ein leistungsstarkes Werkzeug zur Verwaltung Ihrer Benutzer und ihrer Zugriffsrechte. Verwalten Sie Ihre Gruppen in Ihrem Konto, indem Sie sich auf unserer Website hier anmelden.

> Bitte beachten Sie, dass die Gruppenfunktion nur mit Boxcryptor Business und höher verfügbar ist.

Unumkehrbare Operationen wie **Umbennnen**, **Löschen** oder **Eigentumsrechte gewähren** und **entziehen** kann nur der Besitzer der Gruppe (**Eigentümer**) vornehmen. Sie können andere Mitglieder als Eigentümer festlegen und ihnen die Eigentumsrechte auch entziehen. Gruppen können mehrere verschiedene Eigentümer haben.

Vorteile von Gruppen

Neben dem Teilen von Dateien mit einzelnen Konten, können Sie auch **Dateien mit einer Benutzergruppe teilen**. Wenn Sie eine Datei mit einer Gruppe teilen, wird der kryptografische Schlüssel mit einem Gruppenschlüssel verschlüsselt und innerhalb der Datei gespeichert.

Vorteile von Gruppen:

- **Zentrale Verwaltung**: Sie müssen nicht alle Ihre Dateien anklicken, um den Zugang von jemanden zu sehen, zu gewähren oder zu entziehen.
- **Keine Synchronisation notwendig**: Wenn Sie jemanden zu einer Gruppe hinzufügen oder entfernen, werden Änderungen nur auf Ihrem Rechner und unseren Servern durchgeführt. Somit können diese Änderungen deutlich schneller durchgeführt werden. Da sich die Berechtigungen innerhalb der Dateien nicht ändern, ist eine erneute Datei-Synchronisation nicht notwendig.

Einstellungen

App-Schutz

In Boxcryptor für macOS können Sie anstelle des App-Schutzes den **Dateien-Schutz** aktivieren. Der Dateien-Schutz verhindert unbefugten Zugriff auf **Dateien und Ordner im Boxcryptor-Ort** im Finder. Um die Funktion zu nutzen, müssen Sie in der Boxcryptor-App den entsprechenden Schalter „Dateien-Schutz" aktivieren und einen persönlichen, sechsstelligen **Boxcryptor-Code** festlegen. Dieser Code ist **unabhängig von Ihrem Gerätecode und Boxcryptor-Passwort**.

Sie können Ihre Dateien und Ordner nun schützen, indem Sie in der Boxcryptor-App auf **Start** -> **Sperren** klicken. Dadurch werden Ihre Orte vollständig aus dem Finder entfernt, bis Sie wieder entsperren.

Weitere Einstellungsmöglichkeiten:

- **Touch ID (optional)**: Zusätzlich zum Boxcryptor-Code können die je nach Gerät verfügbare biometrische Authentifizierung genutzt werden.
- **Code ändern**: Zur nachträglichen Anpassung des Boxcryptor-Codes.

Für Änderungen an den Einstellungen des Dateien-Schutzes in der Boxcryptor-App ist immer eine erneute Eingabe des sechsstelligen Boxcryptor-Codes notwendig.

Nach zehn erfolglosen Anmeldeversuchen sperrt die Boxcryptor-App den Zugriff auf Ihre Dateien und Ordner unter macOS vollständig. Um danach wieder auf die Daten zugreifen zu können, müssen Sie sich in der Boxcryptor-App selbst ab- und mit Ihrer E-Mail-Adresse sowie Ihrem Boxcryptor-Passwort wieder anmelden.

Anmerkung: Falls es einem erfahrenen Hacker gelingt, Zugriff auf Ihr Betriebssystem zu erlangen, ist es ihm theoretisch möglich die Sicherheits-Funktionen zu umgehen indem er direkt auf die internen Daten der App zugreift. Während die Funktion Ihnen einen verbesserten Schutz Ihrer verschlüsselten Daten auf Ihrem Gerät bieten kann, garantiert sie keine 100%ige Sicherheit gegen erfahrene Angreifer mit Zugriff auf Ihr Betriebssystem. Wir empfehlen den Best Practices für die lokale Sicherheit Ihrer Geräte zu folgen, um eine solche Situation zu vermeiden.

Boxcryptor-Einstellungen

Boxcryptor ist nahtlos in Apples **Finder-App** integriert, sodass die Benutzererfahrung stark von deren Funktionen und Einstellungen abhängt. Einige Einstellmöglichkeiten sind jedoch nur über die Boxcryptor-App vorzunehmen.

Um zu diesen zu gelangen, öffnen Sie die **Boxcryptor-App** und navigieren Sie zu **Einstellungen**. Hier finden Sie Möglichkeiten,

- Dateinamenverschlüsselung zu aktivieren,

- Autostart für Boxcryptor zu aktivieren,
- den Dateien-Schutz einzurichten,
- sowie das Boxcryptor-Konto **abzumelden** und die App auf Werkseinstellungen zurückzusetzen.

Finder Dokumentation

Weitere Informationen zur Funktionsweise und zur Arbeit mit dem Finder finden Sie in Apples eigener Dokumentation.

Boxcryptor-Konto

Ihr Konto verwalten

Sie können Ihr Boxcryptor-Konto verwalten, indem Sie sich auf unserer Website anmelden. Wenn Sie Ihre persönlichen Daten wie Ihren Vornamen, Nachnamen, E-Mail-Adresse oder Ihr Passwort ändern möchten, gehen Sie auf die Seite **Mein Konto**.

Passwort wiederherstellen

Da wir einen Zero-Knowledge-Service anbieten, **können wir Ihr Passwort NICHT zurücksetzen und es Ihnen NICHT nennen**, falls Sie Ihr Passwort vergessen. Jedoch können wir Ihnen anbieten, Ihr Konto vollständig zurückzusetzen.

> ⚠ Wenn Sie Ihr Konto zurücksetzen, werden neue Schlüssel für Ihr Konto erstellt. Das bedeutet, dass Sie unwiederbringlich den Zugriff auf **alle** bereits verschlüsselten Dateien verlieren und aus allen Gruppen entfernt werden.

Sie können Ihr Konto hier zurücksetzen.

Geräte und Sitzungen verwalten

Boxcryptor erfasst alle Geräte und Webbrowser-Sitzungen, die mit Ihrem Konto verknüpft sind. Ein Gerät wird erstellt, wenn Sie sich mit der Boxcryptor-App einloggen. Eine Webbrowser-Sitzung wird erstellt, wenn Sie sich auf unserer Webseite einloggen.

Auf der Geräteübersichts-Seite können Sie Ihre aktuellen Geräte und Websitzungen einsehen und trennen. Das ist praktisch, wenn Sie beispielsweise Ihr Gerät verloren haben oder es gestohlen wurde und Sie den Zugriff auf Ihre Daten unterbinden wollen. Boxcryptor wird die App auf dem getrennten Gerät auf Werkseinstellungen zurücksetzen, sofern eine Internetverbindung besteht.

Hinweis: In der kostenlosen Version können Sie nur zwei Geräte mit Ihrem Konto verknüpfen. Wenn Sie zum Beispiel ein neues Smartphone mit Boxcryptor verwenden möchten, müssen Sie sich zuerst mit dem alten Smartphone abmelden, es auf der Geräte-Übersichtsseite trennen oder Ihre Lizenz erweitern.

Schlüssel exportieren

Sie können Ihre Schlüssel, die auf unseren Servern gespeichert sind, in eine lokale Schlüsseldatei exportieren. Diese Schlüsseldatei kann in Kombination mit einem lokalen Konto genutzt werden, für das keine Verbindung mit unseren Servern notwendig ist. Selbst wenn unser Service für längere Zeit unterbrochen oder komplett abgeschaltet wäre, könnten Sie jederzeit mit Boxcryptor auf Ihre Dateien zugreifen.

Sie können Ihre Schlüssel exportieren, wenn Sie sich auf unserer Webseite mit Ihrem Konto anmelden:

1. Navigieren Sie zu **Mein Konto**.
2. Scrollen Sie herunter zum Bereich **Erweitert** und klicken Sie auf **Schlüssel exportieren**.
3. Sie können Ihre Schlüssel mit Boxcryptor als lokales Konto nutzen.

Um Boxcryptor offline zu nutzen, müssen Sie Ihre Schlüssel nicht exportieren. Wenn Sie sich bereits bei Ihrem Boxcryptor-Konto angemeldet haben, können Sie Boxcryptor problemlos offline nutzen. Ihre Schlüssel sind bereits mit Ihrem Gerät synchronisiert.

Lokales Konto

Der Zweck des lokalen Kontos besteht darin, als Backup-Möglichkeit für Ihre Dateien zu dienen, auch wenn die Boxcryptor-Server nicht verfügbar sind. Dies wird erreicht, indem Ihre Schlüssel lokal in Ihrer eigenen Schlüsseldatei verwaltet werden.

Die Nutzung des lokalen Kontos unterliegt **starken Einschränkungen**:

- Sie können anderen Nutzern keinen Zugang zu Ihren Daten geben.
- Ein Wechsel zwischen Geräten ist schwieriger.
- Gruppen können nicht verwaltet werden.
- Geräte können nicht verwaltet werden.
- Viele Leistungen des Firmenpakets stehen Ihnen nicht zur Verfügung.

Wir empfehlen, ein lokales Konto nicht tagtäglich zu verwenden. Ein lokales Konto dient hauptsächlich als Backup Ihrer Schlüssel.

Eine Schlüsseldatei exportieren

Um ein lokales Konto zu verwenden, müssen Sie zunächst Ihre Schlüssel wie hier beschrieben exportieren.

Eine bestehende Schlüsseldatei öffnen

Version 2 (Standard)

1. Starten Sie Boxcryptor.
2. Klicken Sie auf die **drei Punkte** in der oberen rechten Ecke des Anmeldefensters.
3. Wählen Sie **Lokales Konto**.
4. Wählen Sie **Ich möchte ein lokales Konto verwenden**.
5. Wählen Sie Ihre existierende Schlüsseldatei aus.
6. Melden Sie sich mit Ihrem Passwort an.

Version 3 (File Provider)

1. Doppel-Klicken Sie auf Ihre Schlüsseldatei um Sie mit Boxcryptor zu öffnen.
2. Melden Sie sich mit Ihrem Passwort an.

Wo kann ich mein Konto löschen

Wenn Sie Boxcryptor nicht mehr benutzen möchten, können Sie Ihr Konto löschen. Sämtliche Informationen, inklusive Ihrer Schlüssel, werden dauerhaft von unseren Servern gelöscht. **Vergewissern Sie sich, dass all Ihre Dateien entschlüsselt sind**, bevor Sie fortfahren. Nachdem Ihr Konto gelöscht wurde, gibt es **keine Möglichkeit der Wiederherstellung von Daten**!

> Wir empfehlen vorher einen Schlüsselexport durchzuführen. Dadurch können übersehene verschlüsselte Dateien jederzeit entschlüsselt werden, auch nach Kontolöschung.

Sie können Ihr Konto löschen, indem Sie sich hier anmelden.

Freunde werben

Laden Sie Ihre Freunde zu Boxcryptor ein und machen Sie Ihnen und sich selbst damit eine Freude. Für jede erfolgreiche Empfehlung erhalten jeweils Sie und Ihr Freund ein Monat **Boxcryptor Unlimited Personal kostenlos**. Sowohl Nutzer der kostenlosen als auch Nutzer der Unlimited-Version von Boxcryptor können an dem Empfehlungsprogramm teilnehmen. Nutzer der kostenlosen Version erhalten die zusätzlichen Monate direkt und bei zahlenden Kunden wird das Abonnement um die zusätzlichen Monate verlängert (Erneuerung und Zahlung wird einen Monat später fällig). Sie erhalten ihren **persönlichen Empfehlungslink** nach der Anmeldung auf boxcryptor.com.

Um sich für eine erfolgreiche Empfehlung zu qualifizieren, muss Ihr Freund sein Konto verifizieren und sich einmal anmelden. Das Anmelden muss in einer unserer installierbaren Desktop-Programme auf einem separaten Gerät erfolgen.

Sobald ein Freund Boxcryptor über Ihren Empfehlungslink beigetreten ist, wird er in ihrer Übersicht im Web-Interface angezeigt. Eine Empfehlung kann folgende Zustände haben:

- **Warten auf Überprüfung**: Ihr Freund hat das Konto noch nicht verifiziert. Um dies zu tun, muss er auf den Bestätigungslink klicken, der an seine E-Mail-Adresse gesendet wurde.
- **Warten auf Anmeldung**: Ihr Freund hat sich noch nicht über eine unserer Desktop-Programme in seinem Konto auf einem separaten Gerät angemeldet. Die Anmeldung über ein bereits für eine Empfehlung verwendetes Gerät funktioniert nicht.
- **Warten auf Kontoänderung**: Sie können den Bonus nicht erhalten, da Sie ein Unternehmensnutzer sind. Nur Nutzer der kostenlosen und der Unlimited-Version können den Bonus beanspruchen.
- **Verdient**: Ihr Freund hat alle notwendigen Schritte durchgeführt, damit Sie ihren Bonus beanspruchen können. Klicken Sie auf den Link um ihn einzulösen.
- **Beansprucht**: Sie haben den Bonus beansprucht und erhalten.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) erfordert einen zweiten Faktor beim Anmeldevorgang, um Ihre Identität zu bestätigen. Dieser zweite Faktor ist etwas, das der Nutzer besitzt, wie beispielsweise ein zweites Gerät. Der Vorteil dieser Zusatzverifikation besteht darin, dass ein Angreifer mit Ihrem Passwort allein nichts mehr anfangen kann. Da er keinen Zugriff auf Ihr zweites Gerät hat, kann er sich nicht mit Ihrem Konto anmelden - und Sie bleiben sicher.

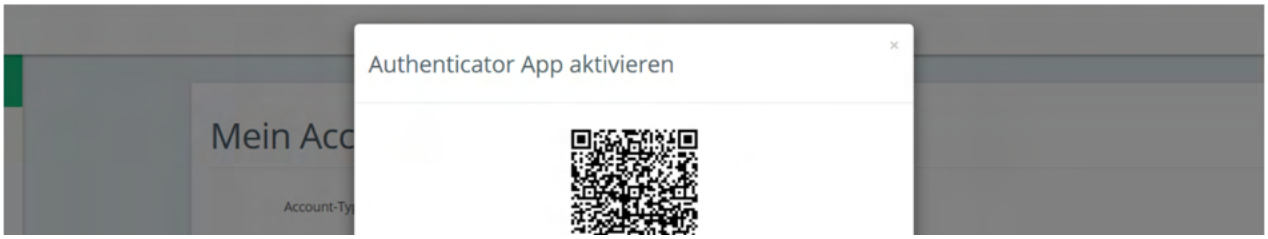
Authenticator-App

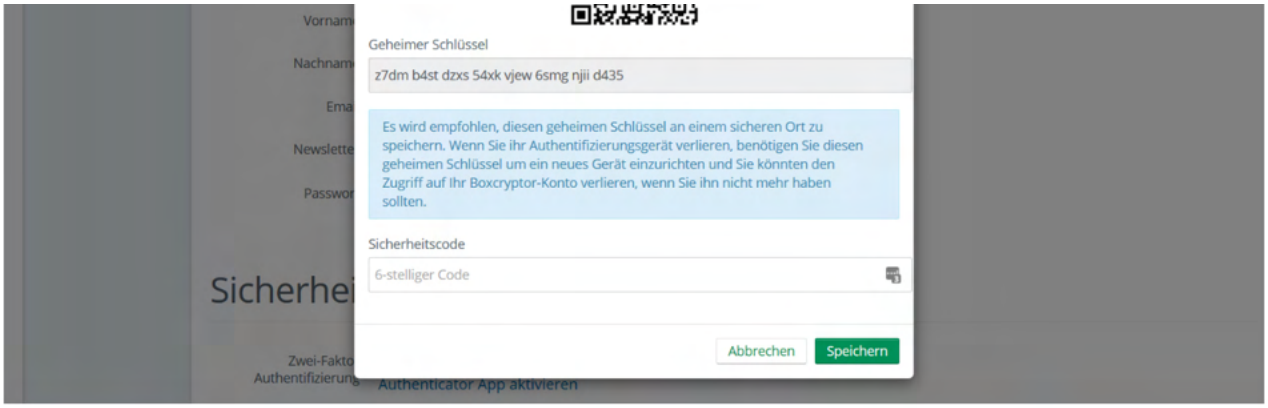
Boxcryptor bietet 2FA mit dem TOTP Protokoll an. Um es zu nutzen, **benötigen Sie eine Authenticator-App** Ihrer Wahl auf Ihrem Smartphone. Als nächstes müssen Sie Ihr Boxcryptor-Konto und Ihre Authenticator-App zur Nutzung von 2FA/TOTP einrichten. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich auf boxcryptor.com an.
2. Navigieren Sie zu **Sicherheit**.
3. Aktivieren Sie **Zwei-Faktor-Authentifizierung -> Authenticator-App**.
4. Scannen Sie den QR-Code mit Ihrer Authenticator-App. Kopieren Sie den **Geheimen Schlüssel** und verwahren Sie ihn an einem sicheren Ort.
5. Um die Einrichtung abzuschließen, geben Sie den 6-stelligen Code aus Ihrer Authenticator App ein.

Von jetzt an müssen Sie sowohl Ihre Zugangsdaten als auch einen 6-stelligen Code aus Ihrer Authenticator App eingeben, um sich anzumelden. Der Code ist zeitbasiert und ändert sich alle 30 Sekunden.

Wichtig: Wenn Sie ihr Smartphone verlieren, können Sie den geheimen Schlüssel nutzen, um Ihre Authenticator-App auf einem anderen Gerät einzurichten. Anschließend können Sie dieses Gerät nutzen, um sich wie gewohnt in Ihrem Konto anzumelden. In diesem Fall empfehlen wir, als nächsten Schritt 2FA zunächst zu de- und dann erneut zu aktivieren. Dieser Schritt stellt sicher, dass das alte Gerät nicht länger zur Anmeldung verwendet werden kann. Bitte verwahren Sie den geheimen Schlüssel sorgfältig. Er sieht so aus:





Es ist möglich, dass bei einem Backup des Mobilgerätes und der anschließenden Wiederherstellung die Einstellungen (Seiten) aus der Authenticator-App verloren gehen. Wir empfehlen daher bereits vorher ein separates Backup der Einstellungen (z.B. durch Sicherung der geheimen Schlüssel oder durch App-interne Backups) zu erstellen. Alternativ können Sie auch einen Security Key als zweiten Backup-Faktor einrichten.

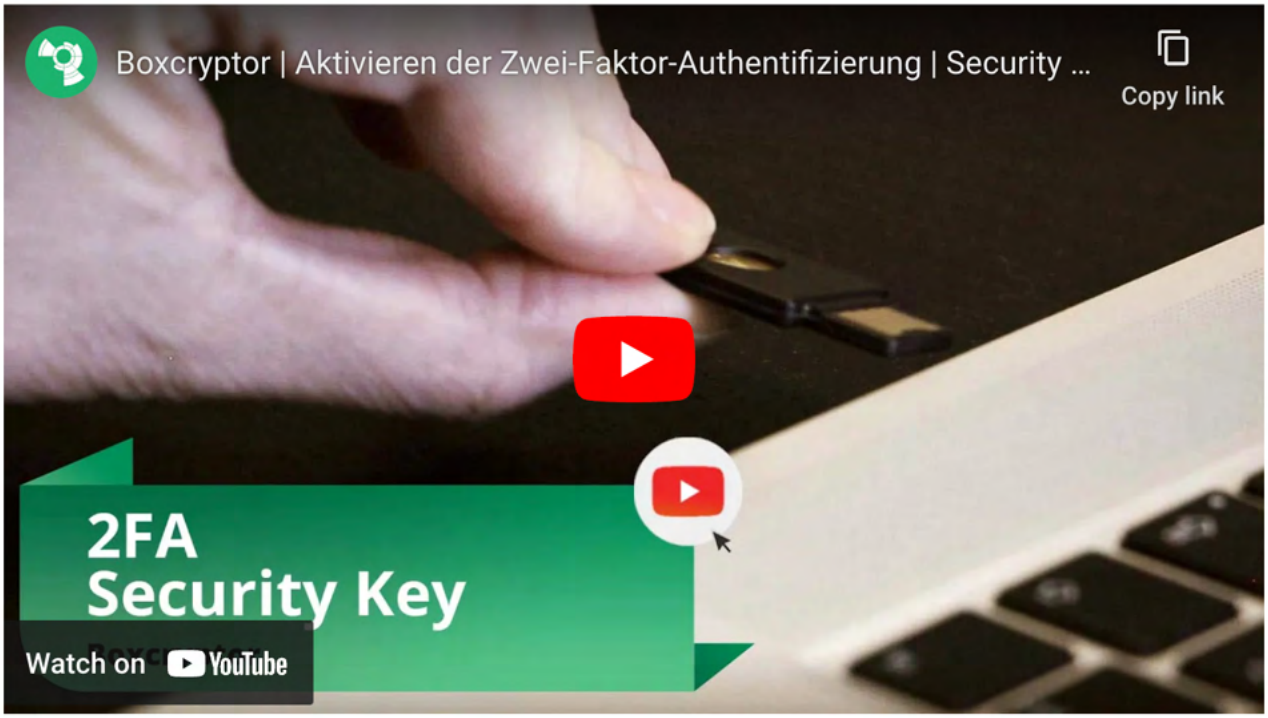
Security Keys

Security Keys nutzen das WebAuthN Protokoll um Ihre Identität durch ein einfaches Tippen auf das Gerät zu bestätigen. Um es zu nutzen benötigen Sie einen Security Key. Anschließend müssen Sie Ihren Security Key in Ihrem Boxcryptor Konto registrieren:

1. Melden Sie sich auf boxcryptor.com an.
2. Navigieren Sie zu **Sicherheit**.
3. Aktivieren Sie **Zwei-Faktor-Authentifizierung -> Security Keys**.
4. Aktivieren Sie **Security Key Hinzufügen** und folgen Sie den Anweisungen auf dem Bildschirm.

Von jetzt an müssen Sie bei der Anmeldung sowohl Ihre Zugangsdaten angeben als auch Ihre Identität über ein Tippen auf Ihren Security Key bestätigen.

Lesen Sie mehr über Security Tokens auf unserem Blog



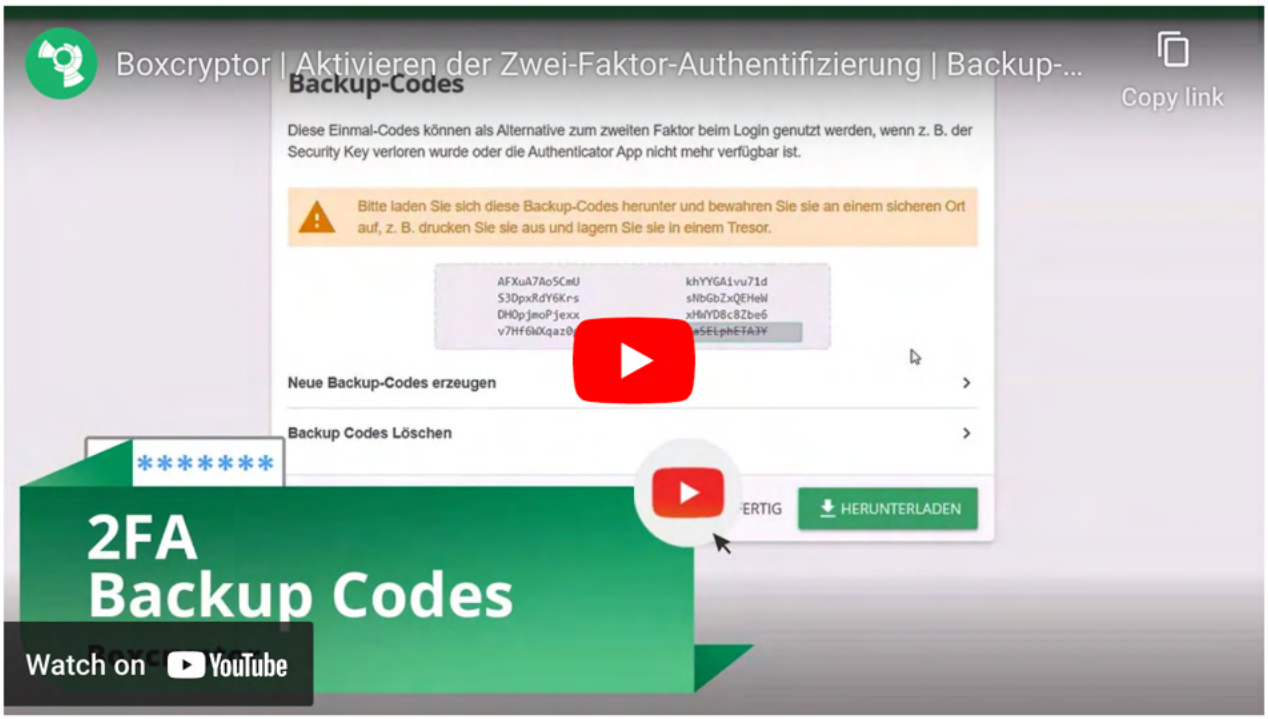
Um ein versehentliches Aussperren zu vermeiden empfehlen wir das Registrieren eines zweiten Security Keys. Nutzen Sie den Ersten für Ihre täglichen Geschäfte und bewaren Sie den Zweiten als Backup auf, falls Sie den ersten verlieren. Alternativ können Sie auch TOTP als zweiten Backup-Faktor einrichten.

Einschränkungen: Security Keys werden derzeit auf Boxcryptor for iOS, Boxcryptor for Android und Boxcryptor Portable **nicht** unterstützt. Bei aktivierter 2FA ist keine Anmeldung möglich. Wenn Sie sich auf boxcryptor.com anmelden, benötigen Sie dazu einen modernen Browser.

Backup-Codes

Backup-Codes sind Einmalcodes, die als Alternative zum zweiten Faktor verwendet werden können, wenn z. B. der Security Key verloren gegangen ist oder das Mobiltelefon mit der Authentifizierungs-App nicht mehr verfügbar ist. Um Ihrem Konto Backup-Codes hinzuzufügen, müssen Sie Ihr Boxcryptor-Konto mithilfe der folgenden Schritte konfigurieren:

1. Melden Sie sich auf boxcryptor.com an.
2. Navigieren Sie zu **Sicherheit**.
3. Aktivieren Sie **Zwei-Faktor-Authentifizierung -> Backup-Codes**. (Diese Option ist nur sichtbar, wenn dem Konto ein mindestens ein zweiter Faktor hinzugefügt wurde.)
4. Jetzt werden die neu generierten Sicherungscodes auf dem Bildschirm angezeigt.



Wir empfehlen, die Sicherungscodes herunterzuladen und sicher aufzubewahren. Um von den Sicherungscodes profitieren zu können, müssen die Codes verfügbar sein, wenn Sie abgemeldet sind.

2FA und die App-Schutz

2FA kommt nur bei Anmeldungen mit Ihrem Boxcryptor-Konto zum Einsatz. Wenn Sie bereits angemeldet sind, wird der zweite Faktor nicht weiter benötigt - selbst wenn Sie den App-Schutz aktiviert haben. Dieses Sicherheitsfeature hilft gegen unauthorisierten Zugriff auf Boxcryptor wenn

Sie **bereits angemeldet sind**. Aus diesem Grunde werden Sie nicht nach Ihrem zweiten Faktor gefragt. Um sicherzustellen, dass Boxcryptor nach Ihrem zweiten Faktor fragt, müssen Sie sich zuerst komplett abmelden.

Einschränkungen: Boxcryptor for Chrome (Beta) unterstützt 2FA **nicht**. Sie werden sich nicht anmelden können, wenn 2FA für Ihr Konto aktiv ist. Es ist jedoch folgender Workaround möglich:

1. Öffnen Sie boxcryptor.com and deaktivieren Sie 2FA.
2. Melden Sie sich im Boxcryptor Client an.
3. Aktivieren Sie 2FA erneut.

FAQ & Fehlerbehebung

Off-Migration Guide: Alle mit Boxcryptor verschlüsselten Dateien entschlüsseln

Da Dropbox mehrere wichtige Assets von der Secomba GmbH i.L. erwirbt, wird Boxcryptor eingestellt und wir werden unseren Service einstellen. Alle Nutzer und Kunden können den Dienst bis zum Ende ihrer Vertragslaufzeit weiter nutzen.

Um von Boxcryptor weg zu migrieren, müssen Sie alle Ihre Dateien entschlüsseln, um den Zugriff darauf zu behalten.

Wenn Sie befürchten, dass Sie den Zugriff auf verschlüsselte Boxcryptor-Dateien verlieren könnten, auf die Sie derzeit keinen physischen Zugriff haben, empfehlen wir dringend, die neuste Boxcryptor Software herunterzuladen und, wie hier beschrieben, Ihre **Schlüssel zu exportieren**. Auf diese Weise können Sie auch nach dem Löschen Ihres Kontos oder dem Abschalten des Boxcryptor-Services später alle Dateien entschlüsseln.

Migration Tips für Unternehmen

- Administratoren können die Schlüssel aller Benutzer exportieren, indem sie in der Benutzerverwaltung in jedem Benutzer `SCHLÜSSEL EXPORTIEREN` auswählen.
- Der Self-Service-Schlüsselexport für Benutzer ist standardmäßig **nicht erlaubt**. Diese Einschränkung kann aufgehoben werden, indem die Richtlinie `Schlüsselexport erlauben` hier aktiviert wird.
- Wenn der **Master Key** aktiviert ist, enthält der Schlüsselexport eines Administratorkontos **alle Schlüssel aller Benutzer mit einem aktiven Hauptschlüssel**. Dies ermöglicht den Gesamtzugriff auf alle Dateien der Organisation.

Das Entschlüsseln Ihrer Dateien ist einfach: Sie können alle Dateien innerhalb des Boxcryptor-Laufwerks kopieren und an einem sicheren Ort einfügen, indem Sie `CMD+C` für die Quelldateien und `CMD+V` im Zielverzeichnis verwenden. Alternativ können Sie die Kontextmenüeinträge des Finders dafür verwenden. Wenn alles entschlüsselt ist, können Sie alle verschlüsselten Quelldateien löschen.

Wenn Sie viele Dateien zu migrieren haben und dabei auf Speicherplatzprobleme stoßen könnten, sollten Sie den Entschlüsselungs- und Löschvorgang in kleineren Teilen ausführen.

Was passiert, wenn es Boxcryptor nicht mehr gibt?

Boxcryptor wurde so entwickelt, dass Boxcryptor auch dann weiterhin funktioniert, selbst wenn die Boxcryptor Server nicht mehr verfügbar sein sollten und Sie noch in Boxcryptor angemeldet sind. Sie benötigen die folgenden Backups, wenn Sie dennoch Vorkehrungen für den Fall treffen möchten, dass die Boxcryptor Server dauerhaft offline sein sollten:

- Exportierte Schlüsseldatei
- Installationsdatei für Boxcryptor

Solange Sie diese Dateien haben, werden Sie immer die Möglichkeit haben, selbstständig auf einem unterstützten Betriebssystem auf Ihre verschlüsselten Dateien zuzugreifen - ohne dass irgendeine Verbindung zu einem Server notwendig wäre. Die exportierte Schlüsseldatei enthält alle für die Entschlüsselung relevanten Schlüssel, die sich in Ihrem Boxcryptor Konto befinden. *Wichtig:* Da durch das automatische Schlüsselmanagement von Boxcryptor mit der Zeit neue Schlüssel hinzukommen können (z.B. wenn Sie mit anderen Benutzern Dateien teilen), wird empfohlen regelmäßig eine neue Schlüsseldatei zu exportieren.

Nachdem Sie Boxcryptor installiert haben, können Sie die exportierte Schlüsseldatei mit einem lokalen Konto verwenden. Erfahren Sie mir über das Exportieren der Schlüssel und über lokale Konten.

Umstellung auf Boxcryptor für macOS v3.x

Mit der Verwendung von Apples File Provider Framework, die in **macOS 12** eingeführt wurden, können wir endlich eine **ganz neue Boxcryptor für macOS-App** anbieten, die sich nahtlos in Apples Mac-Ökosystem integriert, ähnlich wie die Boxcryptor für iOS-App.

Systemanforderungen

Boxcryptor für macOS v3.x ist ab **macOS 12.0** verfügbar.

1. Vorbereitung - FileVault

Mit Boxcryptor sind in der Cloud gespeicherte Dateien immer verschlüsselt und die Verschlüsselung wird immer lokal auf Ihrem Mac durchgeführt. **Nur verschlüsselte Dateien verlassen Ihr Gerät.**

Im Gegensatz zu Boxcryptor für macOS v2.x werden **lokal auf dem Mac gespeicherte Dateien jedoch nicht mehr von Boxcryptor verschlüsselt**, da Apples File-Provider-Plattform technische Einschränkungen mit sich bringt. File-Provider-Apps müssen Dateien im Klartext auf dem lokalen Dateisystem speichern, damit ihr Inhalt von macOS erfasst und dem Benutzer angezeigt werden kann. Dies wirkt sich auf Dateiinhalte und Dateinamen aus.

Hier ist der Verschlüsselungsstatus nach Standort:

- **In der Cloud:** Dateien sind immer durch die Verschlüsselung von Boxcryptor geschützt
- **Auf Ihrem Mac mit FileVault:** Dateien werden durch die Verschlüsselung von FileVault geschützt.
- **Auf Ihrem Mac ohne FileVault:** Dateien sind nicht geschützt (nicht empfohlen)

Wir empfehlen dringend die Verwendung einer lokalen Festplattenverschlüsselung für jeden Mac - unabhängig davon, ob Sie Boxcryptor für macOS v2.x oder die neue v3.x verwenden oder sogar, wenn Sie Boxcryptor überhaupt nicht verwenden. Die Festplattenverschlüsselung ist ein integraler Bestandteil der Sicherheit lokaler Geräte und kann leicht erreicht werden, indem FileVault auf jedem Mac aktiviert wird.

Durch die Verwendung von FileVault sind Dateien, die in Boxcryptor für macOS v3.x verfügbar sind, immer noch durch die Verschlüsselung von FileVault auf der lokalen Festplatte geschützt, obwohl sie als Klartext erscheinen, wenn Ihr Mac in Gebrauch ist. Erfahren Sie hier mehr über FileVault: https://support.apple.com/en-us/HT204837

2. Installation

Boxcryptor für macOS v3.x ist eine native „File Provider"-App, die auf modernen macOS-Betriebssystemen "out-of-the-box" funktioniert. Außerdem nutzt die App jetzt den macOS-Sandboxing-Sicherheitsmechanismus vollständig aus. Sie brauchen nur die neueste Version herunterzuladen und den Standard-Installationsprozess zu befolgen.

3. Clouds und Speicherorte hinzufügen

Boxcryptor für macOS v3.x **umfasst die volle Funktionalität für eine schnelle, reibungslose und sichere Synchronisierung Ihrer Dateien und Ordner.** Um dies zu nutzen, verbinden Sie Ihren Cloud-Anbieter direkt mit der App, indem Sie die folgenden Schritte ausführen:

1. Navigieren Sie zum **Start** Tab
2. Klicken Sie auf **Anbieter hinzufügen...**
3. Wählen Sie den gewünschten Dienst aus
4. Authentifizieren Sie sich mit den Anmeldedaten Ihres Cloud-Anbieters

Ihre Anmeldedaten werden direkt an den von Ihnen gewählten Dienst gesendet, sie werden **nicht** an unsere Server gesendet.

Wenn Sie nicht möchten, dass Boxcryptor Ihre Dateien selbst synchronisiert, können Sie immer noch mit Ihren installierten Sync-Clients arbeiten. Wählen Sie dazu in Ihrer Boxcryptor-App die Option **Lokaler Speicher** und wählen Sie den Sync-Ordner des Clients Ihres Anbieters.

Wie jede File-Provider-App ist Boxcryptor jetzt in `~/Library/CloudStorage` verfügbar, wo ein Sync-Ordner für jeden verbundenen Cloud-Provider erstellt wird. Diese Ordner sind auch **im Finder unter „Speicherort"** zu finden.

4. Boxcryptor für macOS v2.x entfernen

Da Boxcryptor tief in macOS integriert ist und das System keinen eigenen Deinstallations-Mechanismus bereitstellt, folgen Sie bitte diesem Leitfaden, um Boxcryptor vollstandig vom System zu entfernen:

1. Beenden Sie Boxcryptor
2. Offnen Sie **Systemeinstellungen** → **Erweiterungen** →, **Finder Erweiterungen** und deaktivieren Sie Boxcryptor
3. Loschen Sie die folgenden Ordner:

- ~/Library/Application Support/Boxcryptor

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

> ~/Library bezeichnet die Benutzer Library und nicht die System Library.

4. Entfernen Sie die Anwendungs-Einstellungen, indem Sie den folgenden Befehl in der **Terminal App** ausführen: *defaults remove com.boxcryptor.osx*
5. Öffnen Sie die **Schlüsselbundverwaltung** und entfernen Sie alle Eintrage, die mit *com.boxcryptor.osx* beginnen
6. Verschieben Sie **Boxcryptor.app** in den Papierkorb.

5. Sicherheitsrichtlinie zurücksetzen

Wenn Sie die Sicherheitsrichtlinie Ihres Macs aufgrund von Boxcryptor für macOS v2.x auf „Reduzierte Sicherheit" geändert haben, können Sie diese Richtlinie nun wieder auf **„Volle Sicherheit"** zurücksetzen, indem Sie die folgenden Schritte ausführen:

1. Starten Sie Ihren Mac im Wiederherstellungsmodus neu
2. Öffnen Sie Utilities -> Startup Security Utility
3. Wählen Sie Ihr Systemvolume aus, entsperren Sie es und klicken Sie auf Sicherheitsrichtlinie...
4. Wählen Sie Vollständige Sicherheit
5. Starten Sie Ihren Mac neu

6. Sync Clients entfernen

Boxcryptor für macOS v3.x alles, was Sie auf Ihrem Mac benötigen, um mit verschlüsselten Dateien in Dropbox, OneDrive, Google Drive oder jedem anderen unterstützten Cloud-Anbieter zu arbeiten. Sie können den Client Ihres Cloud-Anbieters nun von Ihrem Mac entfernen.

Weitere Informationen

Beschränkungen für Dateinamen und -typen

Aufgrund von technischen Einschränkungen können die folgenden Dateitypen nicht in Boxcryptor gespeichert werden:

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

Falls erforderlich, kann diese Dateitypen-Beschränkung durch das Zippen der Dateien umgangen werden.

Zusätzlich gelten die Beschränkungen für Dateinamen oder -typen der verwendeten Cloud-Speicher.

Spotlight

Ein großer Vorteil der neuen File Provider-API gegenüber dem alten virtuellen Laufwerk ist, dass Spotlight sofort funktioniert, ohne dass Boxcryptor eine besondere Behandlung benötigt. Das bedeutet, dass **Spotlight besuchte Dateien und Ordner in Boxcryptor-Speicherorten automatisch und standardmäßig indiziert.** Spotlight-Unterstützung ist keine optionale erweiterte Einstellung mehr, sondern eine erstklassige Standard-Erfahrung für jeden Benutzer.

Spotlight indiziert die Datei- und Ordner-Metadaten aller Objekte in Boxcryptor-Speicherorten. Dateiinhalte sind nur für heruntergeladene Dateien durchsuchbar, die aufgrund technischer Beschränkungen lokal für die Indizierung verfügbar sind.

Warum ist alles neu?

Ein Hauptgrund für die neue Version von Boxcryptor für macOS ist die Strategie von Apple, Kernel-Erweiterungen von Drittanbietern in macOS zu verbieten, um das Mac-Betriebssystem weiter abzusichern und abzuschotten. Apple hat bereits vor einigen Jahren damit begonnen, Kernel-Erweiterungen von Drittanbietern zu verbieten und ihre Verwendung sukzessive zu erschweren. Während in der Vergangenheit eine Kernel-Erweiterung "on-the-fly" geladen werden konnte, erfordert macOS 10.15 Catalina nun einen Neustart des Systems während des Ladevorgangs.

Heutzutage erfordern Macs mit Apple Silicon Prozessoren zusätzlich die Änderung der Sicherheitsrichtlinien des Macs im Wiederherstellungsmodus, um das Laden von Kernel-Erweiterungen von Drittanbietern zu ermöglichen. Alles deutet darauf hin, dass Kernel-Erweiterungen von Drittanbietern in zukünftigen Versionen von macOS überhaupt nicht mehr funktionieren werden. Die Beibehaltung unseres bestehenden Konzepts mit einem virtuellen Boxcryptor-Laufwerk, das auf einer Kernel-Erweiterung basiert, wäre nicht mehr tragbar.

Aufgrund von Apples Entscheidungen sind wir gezwungen, ein neues Konzept zu entwickeln, wie Boxcryptor für macOS in den kommenden Jahren funktionieren wird. Gleichzeitig freuen wir uns über die neuen Möglichkeiten und Erfahrungen, die diese neue Integration in macOS für Boxcryptor in der Zukunft eröffnet.

Documentation für Boxcryptor 2.x (Legacy)

Diese Dokumentation behandelt unsere neue Boxcryptor für macOS-App, die **macOS >= 12** erfordert. Wenn Sie Hilfe zu unserer alten Boxcryptor-App benötigen, können Sie die Legacy-Dokumentation hier herunterladen.

Wie man ein Debug Log erstellt

Was ist ein Debug Log?

Das Debug Log zeichnet alle internen Ereignisse auf, während Boxcryptor ausgeführt wird. Es unterstützt uns beispielsweise darin, Fehler oder Inkompatibilitäten mit anderen Programmen zu finden.

Enthält ein Debug Log sensible Daten?

Nein. Beim Erstellen eines Debug Logs werden **keine** sensiblen Benutzerinformationen – wie Passwörter, Schlüssel, oder Datei-Inhalte – aufgezeichnet.

Welche Informationen enthält ein Debug Log?

Das Debug Log enthält folgende Informationen.

- Benutzerinteraktionen, wie zum Beispiel Klicks oder Navigation in der App
- Dateioperationen **einschliesslich unverschlüsselter Dateinamen**
- Aktuelle Boxcryptor-Einstellungen
- Kommunikation mit unseren Servern und Cloud-Anbietern
- Systeminformationen wie Betriebssystem oder benötigte Frameworks
- Laufende Programme

Wie erstelle ich ein Debug Log?

1. Öffnen Sie die **Konsole**-App.
2. Geben Sie `com.boxcryptor.` in die obere rechte Suchleiste ein und drücken Sie **Enter**.
3. Klicken Sie auf **Start**.
4. Reproduzieren Sie das Problem, das Sie mit Boxcryptor für macOS haben (Falls Sie Synchronisierungsprobleme haben, warten Sie bitte etwas, sodass der Vorgang hypothetisch abschließen kann).
5. Wechseln Sie zurück zur **Konsole**-App.
6. Klicken Sie auf **Anhalten**.
7. Wählen und kopieren Sie alle Protokolleinträge mit **CMD+A** und **CMD+C**.
8. Öffnen Sie **TextEdit** (oder einen anderen Texteditor Ihrer Wahl).
9. Fügen Sie die Protokolleinträge mit **CMD+V** ein.
10. Speichern Sie die Datei als **boxcryptor.log**.

Was soll ich mit meinem Debug Informationen tun?

Benutzen Sie unser Boxcryptor Hilfe-Fomular um **uns die Datei mit einer detaillierten Beschreibung des Problems zu senden**, oder schreiben Sie an unseren Support Team und hängen Sie die Debug-Informationen an die E-Mail an.

Ich kann mich nicht mit den Boxcryptor-Servern verbinden

Abhängig von Ihren System- oder Netzwerkeinstellungen kann Boxcryptor nicht immer mit unseren Servern kommunizieren. Für die folgenden Probleme gibt es jedoch Lösungsvorschläge:

Fehlermeldungen wie "Keine Verbindung" oder "Synchronisation der Schlüssel fehlgeschlagen":

Bei dieser Fehlermeldung überprüfen Sie bitte, ob Sie eine Internetverbindung mit Ihrem Browser (z.B. Safari) herstellen können. Vergewissern Sie sich, dass der Boxcryptor Server Status hier die Meldung **OK** anzeigt. Eine mögliche Fehlerquelle ist Ihre Proxyeinstellung. Versuchen Sie, die Adresse `api.boxcryptor.com` zu einer Ausnahmeliste hinzuzufügen.

Warnung: Dies ist keine sichere Verbindung

Wenn Sie sich in einer Umgebung befinden, die den Datenverkehr überwacht, können Sie sich möglicherweise nicht mit unseren Servern verbinden. Beispiele für die Behinderung von Boxcryptor aufgrund der Datenüberwachung:

- Antivirenprogramme, die den Internetverkehr schützen
- Öffentliche Hotspots
- Proxy-Server innerhalb von Firmennetzwerken
- **Schadsoftware**

Datenverkehrsüberwachung ist technisch gesehen ein **Man-in-the-Middle-Angriff**. Es ist daher wichtig sicherzustellen, dass Ihr System nicht gefährdet ist. Sie können die Informationen zum mitgelieferten Zertifikat überprüfen, indem Sie in der Fehlermeldung auf **Weitere Informationen** klicken.

Offline arbeiten

Wenn Sie sich schon erfolgreich bei Boxcryptor angemeldet haben, können Sie problemlos an bereits geöffneten oder heruntergeladenen Dateien offline weiterarbeiten. Sie können jedoch keine Boxcryptor-Rechte verändern oder andere Online-Funktionen von Boxcryptor nutzen.

Selbstsignierte Zertifikate für Cloud Provider verwenden

Das Verbinden zu selbst gehosteten WebDAV- oder Owncloud / NextCloud-Instanzen mit **selbstsignierten Zertifikaten** funktioniert nicht immer sofort.

Damit Boxcryptor eine Verbindung zu Ihrem Server herstellen kann, müssen Sie das selbstsignierte Zertifikat auf ihrem Gerät installieren. Weitere Informationen zur Installation finden Sie hier.

Weitere informationen zu Apple's Zertifikatsanforderungen finden sie hier.

> Wenn Sie die Domäne besitzen, können Sie stattdessen ein **freies und vertrauenswürdiges Zertifikat** erstellen. Weitere Informationen finden Sie bei Zertifikatsausstellern wie **Let's Encrypt**.

Ich kann keine Dateien in einen verschlüsselten Ordner verschieben

Das Verschieben von Dateien zwischen unterschiedlich verschlüsselten Ordnern oder in einen neuen verschlüsselten Ordner erfordert immer die erneute Verschlüsselung der Dateien mit einem neuen Schlüssel. Boxcryptor muss das Element herunterladen, entschlüsseln, verschlüsseln und das Element erneut hochladen. Aufgrund der Komplexität haben wir beschlossen, die Option zum Verschieben und Kopieren zwischen verschlüsselten Ordnern zu deaktivieren.

Alternativ können Sie Dateien einfach in den gewünschten Ordner **kopieren** und am Ende die ursprünglichen Elemente löschen.

Wo kann ich Boxcryptor Classic herunterladen?

Boxcryptor Classic ist der Vorgänger von Boxcryptor und wurde eingestellt. Wir empfehlen, Boxcryptor Classic nicht mehr zu benutzen, weil es nicht mehr unterstützt ist und funktioniert nicht mehr auf den neuen Betriebsystemen.

Wenn Sie bereits Kunde von Boxcryptor Classic sind, können Sie es hier herunter laden. Außerdem sollten Sie so schnell wie möglich auf Boxcryptor upgraden. Laden Sie Boxcryptor Classic für Mac OS X hier herunter:
https://www.boxcryptor.com/download/Boxcryptor_Classic_v1.5.415.252_Installer.dmg *Unterstützt Mac OS X 10.7, 10.8, 10.9, 10.10*

Wenn Sie bereits auf Mac OS X >= 10.11 aktualisiert haben und Sie müssen Ihre Boxcryptor Classic Dateien entschlüsseln, können Sie diese „unoffizielle" Version mit Lesezugriff-Support für macOS 10.11 and 10.12 herunterladen:
https://www.dropbox.com/s/wbrygn4x2kgzlsp/Boxcryptor_Classic_v1.5.417.253_Installer.dmg?dl=0

Veraltete Versionen

Wir veröffentlichen regelmäßig neue Versionen von Boxcryptor mit neuen Features, besserer Stabilität und allgemeinen Verbesserungen und stellen veraltete Versionen in regemäßigen Abständen ein. Zum **30. September 2018** wurden die folgenden Versionen eingestellt:

- Boxcryptor for **Windows 2.22.706** und älter
- Boxcryptor for **macOS 2.19.907** und älter

Wenn Sie versuchen eine eingestellte Version zu verwenden, werden Sie Boxcryptor nicht nutzen können und eine der folgenden Fehlermeldungen erhalten:

> Dieser Client ist ungültig oder veraltet. Bitte aktualisieren Sie auf die neueste Version.

> Diese Client ID ist ungültig!

> Dies ist keine sichere Verbindung

> Das Remotezertifikat ist laut Validierungsverfahren ungültig

> Boxcryptor kann keine sichere Verbindung zum Boxcryptor-Server herstellen.

Lösung

Laden Sie die neueste Version von Boxcryptor hier herunter und installieren Sie diese. Danach können Sie Boxcryptor wieder wie gewohnt nutzen.

Sollten Sie die Fehlermeldung **This is no secure connection** weiterhin sehen, liegt eine andere Ursache vor. Weitere Informationen dazu finden Sie hier: **Ich kann mich nicht mit den Boxcryptor-Servern verbinden**.

Ich verwende Windows XP oder Mac OS X 10.14 oder früher

Aktuelle Versionen von Boxcryptor erfordern Windows 7 oder neuer oder macOS 10.15 oder neuer. Da frühere Betriebssystemversionen nicht mehr von Apple oder Microsoft unterstützt werden, empfehlen wir betroffenen Nutzern ihre Betriebssysteme so bald wie möglich auf eine neuere Version zu aktualisieren um weiterhin sicher zu sein.

Die Nutzung von Betriebssystemen, die nicht mehr unterstützt werden, stellt ein hohes Sicherheitsrisiko dar. Für eine sicherheitsrelevante Nutzung müssen Sie Ihr Betriebssystem unbedingt aktuell halten.

Ich kann nicht auf die neueste Version aktualisieren

Hinweis: Wenn Sie **Windows** verwenden sollten, schauen Sie bitte zuerst unter Ich kann Boxcryptor nicht aktualisieren oder entfernen nach.

Falls Sie aus welchem Grund auch immer nicht auf die neueste Version aktualisieren können und somit nicht mehr auf Ihre verschlüsselten Dateien zugreifen können, haben Sie folgende Optionen:

Boxcryptor Portable

Boxcryptor Portable erfordert keine Installation und kann somit auch ohne Administratorenrechte verwendet werden um auf Ihr verschlüsselten Dateien zuzugreifen und diese zu entschlüsseln. Sie können Boxcryptor Portable hier herunterladen.

Schlüsselexport

Sie können Ihre bei uns gespeicherten Schlüssel exportieren und anschließend mit einem lokalen Konto verwenden um sich in Ihrer veralteten Boxcryptor anzumelden ohne eine Verbindung zu unseren Server zu benötigen. Erfahren Sie hier mehr darüber.

Ich kann mich wegen zu vieler verbundener Geräte nicht anmelden

Melden Sie sich an Ihrem Konto auf boxcryptor.com an und entfernen Sie ein Gerät welches Sie nicht länger benötigen. Versuchen Sie dann erneut sich anzumelden.

Manche Dateien lassen sich nicht öffnen

Probleme beim Boxcryptor-Zugriff

> Auf den Desktop Apps zeigen einige Anwendungen oder der Dateibrowser eine Meldung mit dem Wert **`Ungültiger Parameter`** an, wenn versucht wird, eine Datei zu öffnen.

- Boxcryptor ist möglicherweise bei einem falschen Konto angemeldet. → Überprüfen Sie die Kontoinformationen in den Boxcryptor-Einstellungen und vergleichen Sie sie mit den Boxcryptor-Berechtigungen.
- Der Benutzer hat keine Boxcryptor-Berechtigungen für die Datei. → Stellen Sie sicher, dass der Benutzer physischen Zugriff auf die freigegebene Datei hat, die *Boxcryptor-Berechtigungen* korrekt festgelegt und die letzten Berechtigungsänderungen der Datei *synchronisiert* wurden. Erfahren Sie hier, wie Sie Berechtigungen festlegen.

Probleme mit den Dateisystem-Berechtigungen

> Die Datei(en) ist/sind "schreibgeschützt", oder der Benutzer hat keine Berechtigungen.

Ändern Sie die Berechtigungen für das Dateisystem, damit Ihr Benutzer physikalisch auf die Datei(en) zugreifen kann.

Sync-Probleme

> "Bad Padding"-Probleme, leere physische Dateien oder unzugängliche Ordner aufgrund einer leeren Datei "Folderkey.bch".

> Datei öffnen zeigt "Beim Dekodieren ungültige Daten gefunden" und die .bc-Datei ist leer.

> Ordner kann nicht geöffnet werden "Beim Dekodieren wurden ungültige Daten gefunden." wird in den Berechtigungseinstellungen angezeigt.

In der Vergangenheit gab es eine Inkompatibilität mit Dropbox, die zu "falschen" Inhalten für

kleinere Dateien führen konnte, da Dropbox die letzte Dateiänderung nicht synchronisierte.

- Stellen Sie eine ältere Version der beschädigten Datei mithilfe des Dateiversionsverlaufs Ihres Cloud-Speicheranbieters wieder her.
- Wenn es Probleme mit dem Ordner gibt, löschen Sie die leere Datei `Folderkey.bch` und *verschlüsseln* Sie den Ordner *erneut*.

Apple Prozessor-Unterstützung

Am 10. November 2020 stellte Apple eine neue Mac-Hardware mit dem revoluzionären M1 Apple Chip-Prozessor vor, die seit dem 17. November erhältlich ist. Boxcryptor wurde angepasst, um auf der neuen Prozessorarchitektur nativ die maximale Leistung und Batterielaufzeit zu erreichen.

Boxcryptor unterstützt die neuen Apple Silicon-Macs seit der Version 2.39.1119, die am 18.12.2020 veröffentlicht wurde.

Was ist eine FolderKey.bch und eine .bclink Datei?

Es gibt eine Datei mit dem Namen FolderKey.bch in meinem Cloud-Speicher. Was ist das?

Boxcryptor erstellt eine **FolderKey.bch**-Datei wenn ein Ordner verschlüsselt ist. Sie enthält Daten zur Verschlüsselung für den Ordner und hilft Boxcryptor die Verschlüsselungshierarchie zu verwalten. Diese Datei wird im Boxcryptor-Laufwerk nicht angezeigt.

Enthält die Datei sensible Informationen?

Die FolderKey.bch enthält keine sensiblen Informationen. Nur .bc-Dateien enthalten sensible Informationen – und diese sind verschlüsselt.

Was passiert bei Verlust der Datei?

Keine Sorge, Sie verlieren keine Daten oder den Zugriff auf Ihre Dateien. Jede Verschlüsselungsinformation, wird direkt in Ihren verschlüsselten *.bc-Dateien gespeichert.

Der Verlust einer solchen Datei führt dazu, dass Boxcryptor den übergeordneten Ordner nicht mehr als verschlüsselt kennzeichnet. Infolgedessen erben neue Dateien in diesem Ordner die Verschlüsselungseigenschaften nicht.

In meinem Cloud-Speicher befindet sich eine Datei mit dem Namen .bclink. Was ist das?

Die Datei hilft bei der Überprüfung des Kontos, wenn Konten verknüpft werden, um Funktionen wie Whisply zu verwenden.

Wenn die Datei nicht vorhanden ist, hat der Benutzer entweder ein anderes Konto zum Verknüpfen verwendet oder der Synchronisierungsclient ist nicht gestartet oder synchronisiert nicht.

Enthält die Datei sensible Informationen? Kann ich sie löschen?

Die Datei enthält keine sensiblen Informationen. Sie ist nicht notwendig und kann auch gelöscht werden. Allerdings wird sie ggf. automatisch wieder erzeugt.

Account Zugriff bei verlorenem zweiten Faktor (2FA) wiederherstellen

Im Falle eines Verlusts des zweiten Faktors für die Zwei-Faktor-Authentifizierung (2FA), wie z. B. einer **Authentifizierungs-App**, Ihres Mobilgeräts insgesamt, Ihres **Sicherheitsschlüssels** oder anderer Hardware, können Sie sich nicht mehr bei Ihrem Boxcryptor-Konto anmelden.

Möglichkeiten, den Zugriff auf Ihr Konto wiederherzustellen:

Den geheimen Schlüssel aus der Ersteinrichtung erneut anwenden

Wenn Sie noch Ihren geheimen Schlüssel aus der Ersteinrichtung der Authenticator-App haben, können Sie ihn einfach erneut zu Ihrer Authenticator-App Ihrer Wahl hinzufügen. Neben der QR-Code-Scanmethode bieten diese Apps normalerweise eine "manuelle" Möglichkeit, ein Konto mit zeitbasiertem Einmalpasswort (TOTP) hinzuzufügen.

Als Referenz sieht der geheime Schlüssel ähnlich aus wie:

> mzwe wocd mj3d qr3f njjw g2cm grqw cvli

Einen Gerätecode verwenden

Wenn Sie kürzlich noch mit den Apps **Boxcryptor für Windows** oder **Boxcryptor für macOS** gearbeitet haben und weiterhin angemeldet sind, können Sie diese Geräte stattdessen als zweiten Faktor verwenden.

Der Anmeldeprozedur bietet Ihnen dann die zusätzliche Option „Gerätecode verwenden“ an. Wenn Sie darauf klicken, erhalten Sie von unseren Apps eine temporäre 8-stellige PIN, die 5 Minuten lang gültig ist.

> Bitte stellen Sie vorher sicher, dass Ihr Boxcryptor-Client auf dem neuesten Stand ist. Sie können die neueste Version immer hier herunterladen.
> Stellen Sie außerdem sicher, dass der Boxcryptor-Client gestartet und **entsperrt** ist, bevor Sie einen Gerätecode anfordern.

Einen Backup-Code einsetzen

Sobald Sie Ihren zweiten Faktor eingerichtet haben, werden **Backup-Codes** generiert und Ihnen angezeigt. Sie können diese **einmaligen** Codes anstelle Ihres zweiten Faktors verwenden.

Sollten Ihnen die Einmalcodes ausgehen, können Sie hier neue Codes generieren.

Keine der oben genannten Methoden sind möglich

Wenn Sie immer noch nicht auf Ihr Konto zugreifen können, können Sie uns auch kontaktieren, um die Zwei-Faktor-Authentifizierung zu deaktivieren.

Wir benötigen jedoch einen eindeutigen Nachweis, dass Sie der rechtmäßige Eigentümer dieses Kontos sind.

Die Identifizierung erfolgt per Video-Live-Chat, Sie benötigen hierzu folgende Dinge:

1. Ein Gerät mit einem installierten **Browser** und einer **funktionierenden Kamera**.
2. Eine **Identifikation** Ihrer **Person** (Personalausweis, Reisepass oder Führerschein).
3. Die **gültige E-Mail-Adresse** Ihres **Boxcryptor-Kontos**.

Um einen Termin auszuwählen, gehen Sie bitte auf unsere **Buchungsseite**.

Bitte geben Sie eine gültige E-Mail-Adresse an, da diese für eine Kalendereinladung, weitere Anweisungen und einen Link zur Teilnahme an einem Meeting verwendet wird.

Als Video-Chat-Plattform verwenden wir **Microsoft Teams**. Sie **brauchen dort kein Benutzerkonto**. Auf Desktop-Rechnern reicht ein moderner Browser (Chrome, Edge oder Safari) aus. Für andere Browser oder Mobilgeräte müssen Sie möglicherweise die Microsoft Teams-App herunterladen:

iPhone und 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

Ungültige Codes der Authenticator App

Sollten Sie trotz funktionierender Authenticator App keine gültigen Codes generieren können, liegt dies höchstwahrscheinlich an einer abweichenden Urzeit auf einem der beteiligten Systeme.

Da diese TOTP Codes nur 30 Sekunden gelten, können bereits Abweichungen zur Realzeit von nur wenigen Sekunden zu Anmeldeproblemen führen.

Sie können die Synchronisation auf allen beteiligten Geräten überprüfen, in dem Sie folgende Website aufrufen: https://time.is

Beträgt der Zeitunterschied mehr als ein paar Sekunden, empfehlen wir Ihnen, die automatische Zeitsynchronisation Ihrer Geräte einzurichten oder ggf. neu durchzuführen.

Sonstiges

Wartungsfenster

Um unseren Service ständig zu verbessern und unsere Server auf dem aktuellen Stand zu halten, wird unsere Infrastruktur regelmäßig gewartet. Arbeiten, die Auswirkungen auf die Verfügbarkeit unseres Service haben könnten, werden wöchentlich im folgenden Wartungsfenster durchgeführt:

Jeden Montag, 00:00 - 02:00 UTC+1 (4pm - 6pm UTC-7)

Wir versuchen, die bestmögliche Verfügbarkeit unseres Service zu gewährleisten, aber während dieser zwei Stunden kann der Zugang zu unseren Servern eventuell gestört oder nicht möglich sein. Boxcryptor wurde so konzipiert, dass für die reguläre Nutzung unserer Software Zugang zu unseren Servern nicht notwendig ist. Wie in unserem Technischer Überblick (*Warum und in welchen Fällen Boxcryptor eine Internetverbindung benötigt*) beschrieben, erfordern nur folgende Aktionen eine aktive Verbindung zu unseren Servern:

- Ein Boxcryptor-Konto erstellen
- Ein neues Gerät einrichten
- Zugang zu einer Datei oder einem Verzeichnis teilen
- Konto synchronisieren

Wenn Sie auf Ihrem Gerät bereits mit Ihrem Boxcryptor -Konto angemeldet sind, haben Sie immer Zugriff auf Ihre verschlüsselten Dateien, unabhängig von Ihrer Internetverbindung oder der Verfügbarkeit unserer Server.

Changelog

Version 3.12.379 (2022-11-24)

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

Version 3.11.318 (2022-10-17)

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

Version 3.10.314 (2022-10-14)

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

Version 3.9.264 (2022-09-20)

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

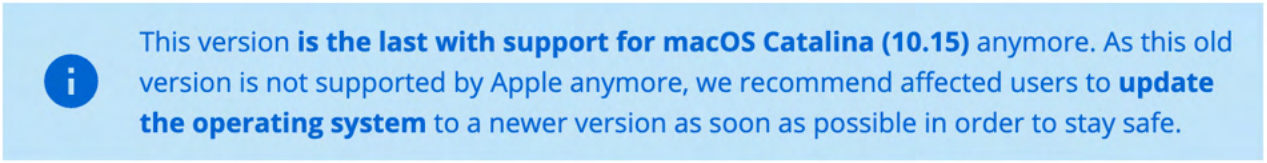
Version 3.8.254 (2022-09-08)

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

Version 2.47.1885 (2022-10-19)

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

Version 2.46.1667 & 2.46.1668 (2022-03-21)



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

Version 2.45.1654 & 2.45.1655 (2022-03-14)

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

Version 2.44.1601 & 2.44.1602 (2022-01-31)

- Added: Support for OneDrive for Mac v22 with updated Files On-Demand experience

- Added: Support for Box Drive on macOS File Provider Extension mode
- Fixed: Opening PDF files in Adobe Acrobat DC may fail on macOS 12.1
- Changed: Removed path length restriction for Microsoft Excel
- Minor bug fixes and improvements

Version 2.43.1464 & 2.43.1465 (2021-10-14)

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

Version 2.42.1436 & 2.42.1437 (2021-09-20)

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

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

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

Version 2.41.1307 & 2.41.1308 (2021-05-31)

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

Version 2.40.1233 & 2.40.1234 (2021-03-29)

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

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

Version 2.39.1119 (2020-12-18)

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

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

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

Version 2.38.1090 (2020-12-01)

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

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

Version 2.38.1086 (2020-11-30)

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

Version 2.37.1043 (2020-11-04)

- Minor bug fixes and improvements

Version 2.36.1042 (2020-10-16)

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

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

- Changed: Sign out is now part of the account preferences
- ○ Changed: Updated BCFS to v3.11.2
- Fixed: Administrators could not change permissions to other groups using the Master Key
- Fixed: Local privilege escalation
- Minor bug fixes and improvements

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

Version 2.35.1024 (2020-06-22)

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

Version 2.34.1023 (2020-06-09)

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

Version 2.33.1015 (2020-02-24)

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

Version 2.32.1010 (2019-12-16)

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

Version 2.31.1006 (2019-11-07)

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

Version 2.30.1004 (2019-10-07)

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

Version 2.29.1001 (2019-09-25)

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

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

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

Version 2.28.995 (2019-07-10)

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

Version 2.27.977 (2018-12-18)

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

Version 2.26.964 (2018-09-06)

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

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

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

Version 2.25.954 (2018-07-31)

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

Version 2.24.941 (2018-06-14)

- Minor bug fixes and improvements

Version 2.23.939 (2018-05-24)

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

Version 2.22.933 (2018-04-19)

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

Version 2.21.923 (2018-02-28)

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

Version 2.20.918 (2018-02-13)

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

Version 2.19.907 (2017-12-13)

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

Version 2.18.902 (2017-12-12)

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

Version 2.17.892 (2017-11-23)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Changed: New provisioning profile valid until 2035
- Minor bug fixes and improvements

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

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

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

- Minor bug fixes and improvements

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

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

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

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

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

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

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

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

- Fixed: Spotlight does not include results from Boxcryptor drive in v2.3 versions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Minor bug fixes and improvements.

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

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

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

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

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

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

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

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

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

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

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

- Minor bug fixes and improvements.

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

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

- Fixed: Deadlock of the Boxcryptor disk when running an executable from the disk.
- Improved: Updated BCFS 3.0.4

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

on full iCloud support also on mobile devices which will be available in the next version of Boxcryptor for iOS (ETA in January).
- Fixed: Problems when using Wuala
- Fixed: Boxcryptor disk can deadlock on accessing symlinks in the Boxcryptor disk which have a target in the Boxcryptor disk.
- Minor bug fixes and improvements

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

- Fixed: Issue with desktop alias creation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Minor bug fixes and improvements

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

- Initial Release

Netzwerkzugriff

Boxcryptor setzt voraus, dass bestimmte Server über das Internet erreichbar sind. Falls Sie Netzwerkbeschränkungen verwenden, stellen Sie bitte sicher, dass Verbindungen von Boxcryptor zu folgenden Domänen, Ports, Protokollen und IP-Adressen erlaubt sind:

```
Domäne: www.boxcryptor.com
Port: 443
Protokoll: HTTPS
IP-Adressen: 136.243.125.201, 148.251.224.98, 188.40.161.200
```

```
Domäne: api.boxcryptor.com
Port: 443
Protokoll: HTTPS
IP-Adressen: 136.243.125.202, 148.251.224.99, 188.40.161.201
```

```
Domäne: whisp.ly
Port: 443
Protocol: HTTPS
IP-Adressen: 188.40.161.203
```

Falls Sie unser LDAP / Active Directory Synchronisations-Feature verwenden, stellen Sie bitte sicher, dass Ihr Verzeichnisserver von den folgenden Subnetzen aus erreichbar ist: `148.251.224.96/28`, `136.243.125.192/28`, `188.40.161.192/28`.

Bitte beachten Sie, dass sich diese Domänen und auch IP-Adressen in der Zukunft ändern können.

Open-Source-Lizenzen

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