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. Außerdem werden typische Cloudeigenschaften, wie Dateiversionierung oder selektive Synchronisation ebenfalls unterstützt.

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.
- Boxcryptor ist **kein Synchronisationsdienst**. Das bedeutet, dass Boxcryptor auf Windows und macOS 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

Systemvorraussetzungen: Benötigt macOS 10.15 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.

Um Boxcryptor auf Ihrem Mac zu installieren, folgen Sie diesen Anweisungen:

1. Installieren Sie die Desktop-Anwendung Ihres Cloud-Anbieters.
2. Laden Sie Boxcryptor für macOS herunter.
3. Öffnen Sie die Installationsdatei.
4. Ziehen Sie das Boxcryptor-Icon per Drag & Drop in das Anwendungsverzeichnis.

Erforderliche Systemerweiterung
Boxcryptor 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.

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.

Ein Boxcryptor-Konto erstellen

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

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

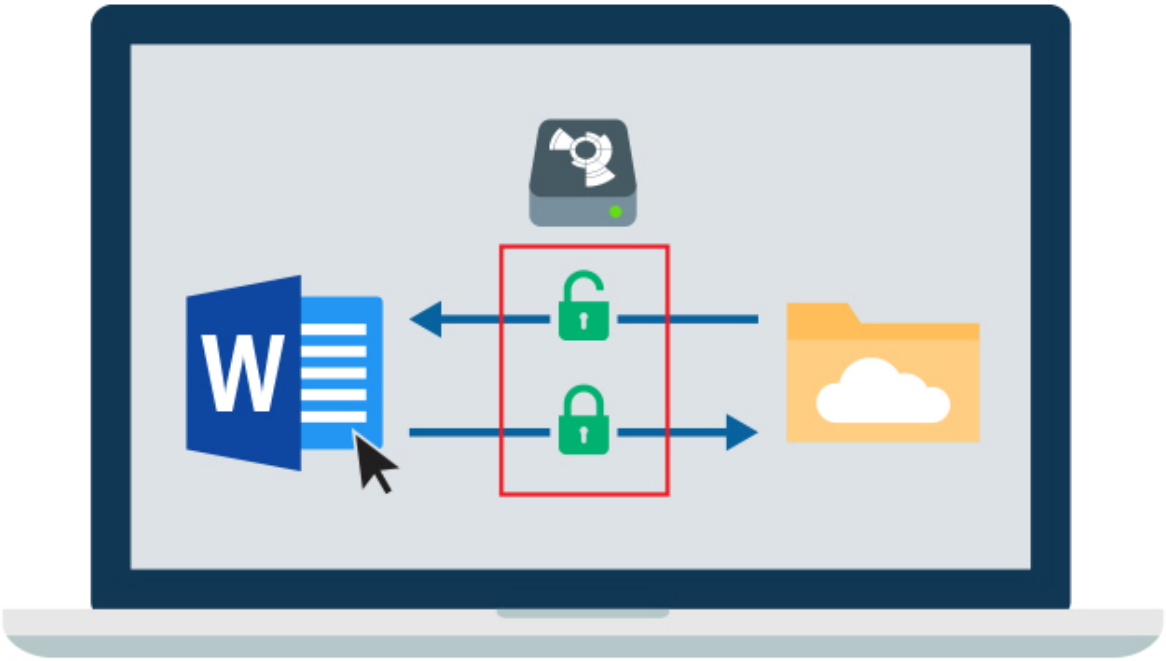
Wählen Sie ein Passwort, das Sie sich merken können oder bewahren Sie das Passwort an einem sicheren Ort auf, wie zum Beispiel einem Passwortmanager. Boxcryptor folgt dem Zero-Knowledge-Prinzip, daher können wir Ihr Passwort **nicht** zurücksetzen.

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

Entdecken Sie Boxcryptor

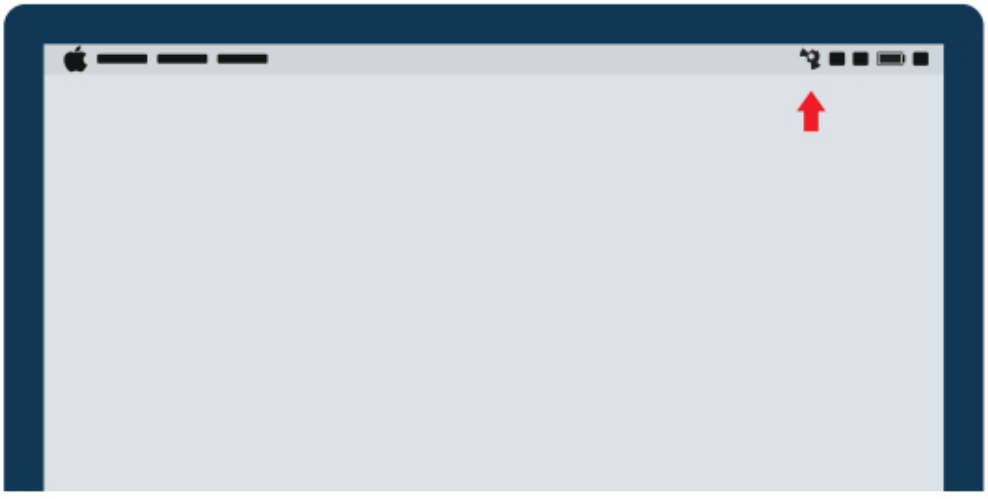
Nachdem Sie Boxcryptor installiert und sich mit Ihrem Boxcryptor-Konto angemeldet haben, können Sie auf das **Boxcryptor-Laufwerk** zugreifen.

Boxcryptor fügt automatisch alle installierten Cloud-Anbieter zum Laufwerk hinzu. Ab jetzt finden Sie hier all Ihre Cloud-Speicher. Das Laufwerk ist wie eine Schicht, die über Ihre vorhande Dateien gelegt wird. Es ermöglicht Ihnen, Ihre verschlüsselten Dateien unmittelbar zu öffnen, zu ändern und zu speichern.



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

Hinweis: Sie erreichen Ihr Boxcryptor-Laufwerk auch durch Doppelklick auf das Boxcryptor-Symbol in der Menüleiste, in der Seitenleiste im Finder oder auf dem Desktop.



Ihr erster verschlüsselter Ordner

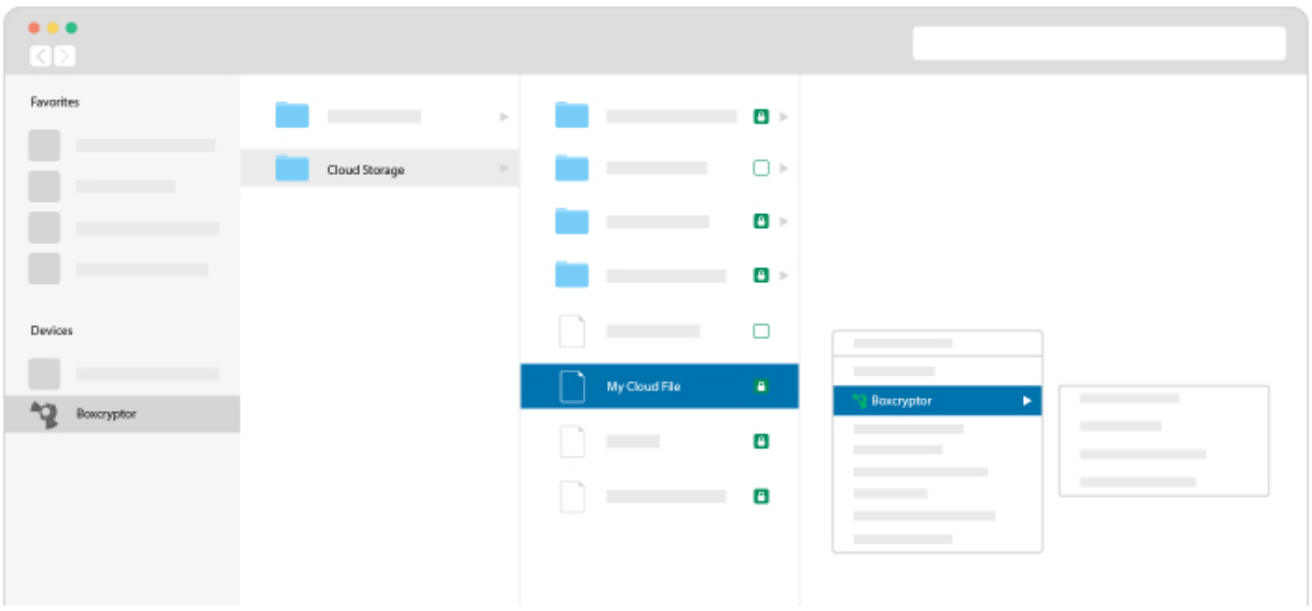
Alle Dateien und Ordner, die Sie einem **verschlüsselten Ordner** in Boxcryptor hinzufügen, werden **automatisch verschlüsselt**. So gehen Sie vor, wenn Sie Boxcryptor das erste Mal verwenden und noch keine Dateien in Ihrer Cloud haben.

1. Öffnen Sie Ihr **Boxcryptor-Laufwerk**.
2. Öffnen Sie darin den Ordner Ihres Cloud-Anbieters.
3. **Rechtsklick** in den Ordner → **Neuer Ordner**.
4. Wenn Sie einen verschlüsselten Ordner erstellen möchten, bestätigen Sie mit einem Klick auf **Ja**.
5. Fügen Sie dem Ordner Dateien hinzu. Alle Dateien werden automatisch verschlüsselt.

Wie man bestehende Dateien verschlüsselt

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

1. Wählen Sie Ihr **Boxcryptor-Laufwerk**.
2. **Rechtsklick** auf eine Datei oder einen Ordner → **Boxcryptor** → **Verschlüsseln**.
3. Warten Sie, bis der Sync-Client Ihres Cloud-Anbieter **alles synchronisiert hat**.



Um bei der Verschlüsselung bestehender Ordner Synchronisierungskonflikte zu vermeiden, erstellt Boxcryptor einen neuen Ordner mit dem Suffix *_encrypted* und schiebt Ihre bestehenden Dateien in diesen neuen Ordner. Das Suffix kann ohne Bedenken entfernt werden, nachdem der Ordner von Ihrem Cloud-Anbieter synchronisiert wurde.

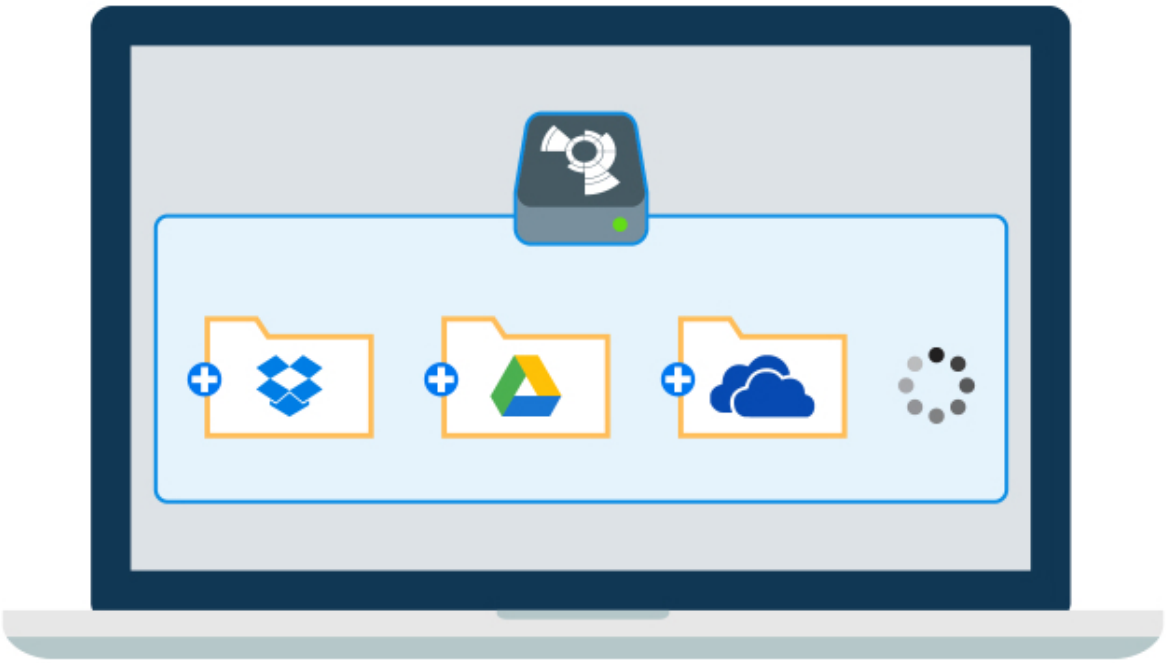
Verwalten Sie Ihre Clouds und Speicherorte

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

Cloud-Speicher

Boxcryptor ist eine **zusätzliche Sicherheitsebene** für Ihren Cloud-Speicher. Wir kümmern uns um die Verschlüsselung, während die Software des Cloud-Anbieters Ihre Dateien snychronisiert. Deshalb **muss die jeweilige Desktop-Anwendung des Cloud-Anbieters auf Ihrem Computer installiert sein**.

Die meisten Cloud-Speicher werden automatisch von Boxcryptor erkannt und als Speicherort zu Ihrem Boxcryptor-Laufwerk hinzugefügt. Falls Ihr Cloud-Speicher nicht automatisch erkannt wird, können Sie ihn manuell hinzufügen.



Individuelle Speicherorte können über die Speicherorte-Einstellungen aktiviert und deaktiviert werden. Klicken Sie mit der rechten Maustaste auf auf **Boxcryptor-Symbol in der Taskleiste** → **Einstellungen** → **Speicherorte** und aktivieren oder deaktivieren Sie die Speicherorte nach Ihrem Belieben.

Hinweis: Nutzer der kostenlosen Version können nur einen Speicherort hinzufügen. Wenn Sie mehrere Speicherorte verwenden möchten, upgraden Sie bitte Ihre Lizenz.

Dropbox

Dropbox ist mit macOS 12.3 nicht kompatibel, weil der Dropbox-Client macOS 12.3 noch nicht vollständig unterstützt. Wenn Sie sich für ein Update auf macOS 12.3 entscheiden, **werden Sie Problem beim Öffnen von reinen Onlinedateien** in Dropbox mit manchen Anwendungen von Drittanbietern haben. Dropbox lädt diese nicht mehr automatisch herunter.

Die neueste Version von Boxcryptor enthält eine Gegenmaßnahmen für diese Inkompatibilität, so dass das Öffnen von verschlüsselten, reinen Onlinedateien in Boxcryptor wie erwartet funktioniert. **Wir empfehlen dringend, unter macOS 12.3 die Boxcryptor-Version 2.46.1668 oder neuer zu verwenden.** Die neueste Version von Boxcryptor für macOS kann hier heruntergeladen werden.

Kennen Sie schon die nächste Generation von Boxcryptor für macOS? Diese benötigt keinen Dropbox-Client und unterstützt macOS 12.3 vollständig. Erfahren Sie mehr darüber in unserem Blog.

OneDrive

Aufgrund technischer Einschränkungen des neuen OneDrive-Clients mit aktualisiertem Files On-Demand-Erlebnis kann Boxcryptor verschlüsselte Nur-Online-Verfügbare-Dateien nicht beim ersten Versuch öffnen. Nur-Online-Verfügbare-Dateien sind nur online verfügbar und nicht lokal auf Ihrem Mac.

Der erste Versuch, eine solche verschlüsselte Datei in Boxcryptor zu öffnen, schlägt daher immer fehl. Gleichzeitig zeigt Boxcryptor eine entsprechende Meldung an und stößt automatisch den Download der Datei an. **Nachdem die Datei von OneDrive heruntergeladen wurde, kann sie beim zweiten und den folgenden Versuchen wie gewohnt geöffnet werden, so lange sie lokal auf dem Mac verfügbar ist.**

Obwohl Sie eine Fehlermeldung erhalten, wenn Sie versuchen, eine verschlüsselte Nur-Online-Verfügbare-Datei zum ersten Mal zu öffnen, **sind Ihre verschlüsselten Daten nie gefährdet.** Das aktualisierte Files On-Demand-Erlebnis von OneDrive unterstützt das gleichzeitige Herunterladen und Öffnen verschlüsselter Dateien leider nicht, so dass Boxcryptor diese Aktionen getrennt voneinander durchführen muss. Für lokal verfügbare Dateien arbeitet Boxcryptor ohne Einschränkungen mit OneDrive zusammen.

Wir arbeiten an einer komplett überarbeiteten Boxcryptor für macOS-Version, die nicht mehr vom OneDrive Sync Client abhängig sein wird. Sie können hier mehr darüber erfahren.

Google Drive

Boxcryptor erkennt automatisch sowohl Ihre **gespiegelten** als auch **gestreamten** Speicherorte von Google Drive. **Alle zusätzlichen gesicherten Ordner werden nicht automatisch hinzugefügt.**

Auf anderen Geräten sind nur Inhalte verfügbar, die über den Tab **Google Drive** synchronisiert wurden. Ordner aus **Mein Computer** sind auf anderen Computern sowie in den mobilen Boxcryptor-Apps nicht zugänglich. Wenn Sie Dateien in einem gesicherten Ordner verschlüsseln möchten, können Sie ihn manuell als

benutzerdefinierter Speicherort hinzufügen.

Geteilte Ablagen werden derzeit nur in **gestreamten** Speicherorten unterstützt.

Maximale Länge eines Dateinamen

Obwohl Google Drive selbst die maximale Länge eines Dateinamen nicht begrenzt und Dateinamen jeglicher Größe **von einem Mac nach Google Drive** synchronisiert, ist die maximale Dateinamenlänge beschränkt wenn eine Datei oder ein Ordner **von Google Drive zu einem Mac** synchronisiert wird.

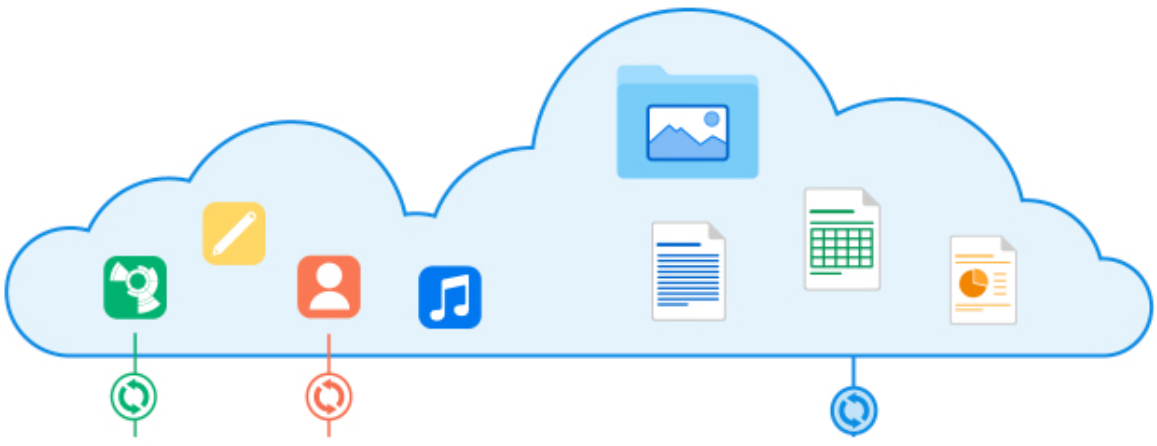
Während **gespiegelte** Speicherorte dabei eine maximale Dateinamenlänge von **255 Bytes** haben, erlauben **gestreamte** Speicherorte nur bis zu **250 Bytes** für einen Dateinamen. Wenn ein Dateiname dieses Limit überschreitet, wird die Datei zwar von Google Drive synchronisiert - allerdings nur mit einem gekürzten und abgeschnittenen Dateinamen damit das Limit eingehalten wird. Bitte beachten Sie, dass die Länge nicht anhand der Anzahl an Buchstaben beschränkt ist, sondern an der Anzahl an Bytes, die für den Namen benötigt werden. Ein von Boxcryptor für die Dateinamenverschlüsselung verwendeter Buchstabe kann bis zu 4 Byte beanspruchen.

Falls ein verschlüsselter Dateiname abgeschnitten wird, kann dieser von Boxcryptor nicht mehr erfolgreich entschlüsselt werden, da der vollständige Dateiname für die Entschlüsselung erforderlich ist. In einem solchen Fall **müssen Sie den Dateinamen kürzen**, so dass dieser die Beschränkungen von Google Drive einhält und nicht durch Google Drive modifiziert wird.

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.

Die Tatsache, dass es ein iCloud Drive (ein typischer Cloud-Anbieter) und eine iCloud gibt (wo all Ihre Apps und der dazugehörige Cloud-Speicher von Apple verwaltet werden), macht die plattformübergreifende Einrichtung der Verschlüsselung etwas komplizierter in Vergleich zu anderen Clouds. Aber wenn iCloud in Kombination mit Boxcryptor einmal eingerichtet ist, ist die Arbeit mit den Daten genauso einfach wie auf anderen Plattformen.



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

iCloud Drive verschlüsseln und alle Daten auf Mobil- und Desktopgeräten zur Verfügung stellen

Wenn Sie möchten, dass Ihre verschlüsselten Daten auf all Ihren Geräten verfügbar sind, dann gehen Sie bitte wie folgt vor:

1. Installieren Sie Boxcryptor auf Ihren iPhone oder iPad und auch auf Ihren Desktopgeräten.
2. Stellen Sie sicher, dass Sie in iCloud auf allen Geräten angemeldet sind.
3. Fügen Sie den **iCloud** Anbieter in Boxcryptor für iOS hinzu.
4. Laden Sie eine verschlüsselte Datei via Boxcryptor in die **iCloud** für iOS hoch.
5. Apple wird daraufhin ein Boxcryptor-Verzeichnis in ihrer Cloud erzeugen.
6. Öffnen Sie Boxcryptor auf dem Desktop und gehen Sie unter macOS auf die **iCloud**-Adresse oder **iCloud Drive** → **Boxcryptor** unter Windows. Dort werden Sie die verschlüsselte Datei vom iPhone oder iPad wieder finden.
7. Um Dateien von einem Mac oder PC auf einem iPhone oder iPad zur Verfügung zu stellen, bewegen oder kopieren Sie die Dateien oder Verzeichnisse in die vorher genannten Verzeichnisse. Dann werden Sie die Daten sowohl mobil aus auch auf dem Desktop zur Verfügung haben.

Nur in iCloud gespeicherte Dateien

Aufgrund technischer Einschränkungen müssen Dateien heruntergeladen und für Boxcryptor auf dem Mac verfügbar sein. Dateien, die nur in iCloud verfügbar und nicht auf dem Mac gespeichert sind, sind im Boxcryptor Laufwerk nicht verfügbar. Solche Dateien müssen erst in iCloud Drive heruntergeladen werden, bevor sie im Boxcryptor-Laufwerk erscheinen.

Ich kann mein iCloud Laufwerk nicht aktivieren

Bevor Sie Ihre iCloud als Laufwerk aktivieren können, **fügen Sie bitte iCloud in Ihrer Boxcryptor für iOS App hinzu**. Laden Sie eine kleine Testdatei hoch, damit das Apple-Dateisystem einen Boxcryptor-Ordner erstellt.

Netzlaufwerke und USB-Geräte

Entfernbare USB-Laufwerke werden von Boxcryptor ebenfalls automatisch erkannt.

Netzlaufwerke werden derzeit noch nicht automatisch von Boxcryptor erkannt. Sie können Netzlaufwerke als einen eigenen Pfad, wie unten beschrieben, hinzufügen.

Wie kann man die automatische Erkennung von entfernbaren Laufwerken deaktivieren?

Sie können diese Funktion deaktivieren, indem Sie die versteckte Einstellung **autoDetectRemovableDrives** verwenden.

Benutzerdefinierte Speicherorte

Falls Ihre bevorzugte Cloud nicht als unterstützter Anbieter aufgeführt ist oder falls Sie einen bestimmten Ordner auf Ihrem Mac verschlüsseln möchten, können Sie das ebenfalls tun:

Klicken Sie auf das **Boxcryptor-Symbol in der Menüleiste** → **Preferences** → **Locations** → + und wählen Sie dann den zu verschlüsselnden Ort aus.

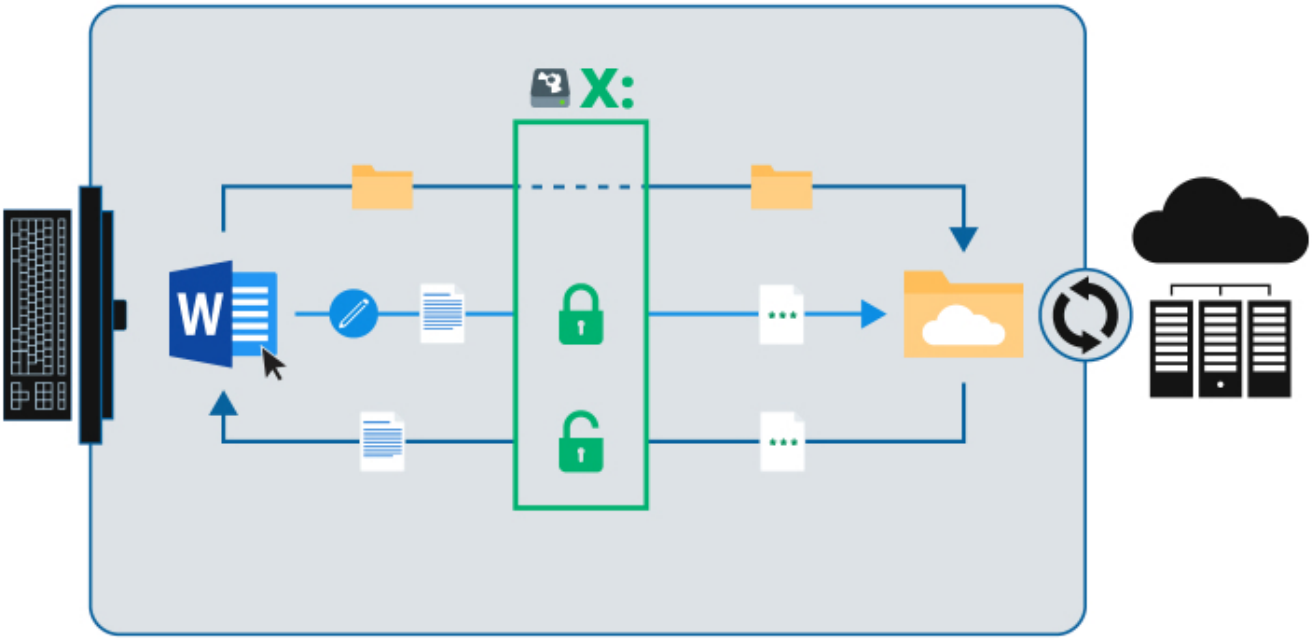
Falls Ihr gewählter Speicherort kein Ordner ist, der von einem Cloud-Anbieter synchronisiert wird, wird nichts in die Cloud hochgeladen. Die Daten bleiben lokal auf Ihrem Mac, wie jeder andere Ordner, aber verschlüsselt.

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.



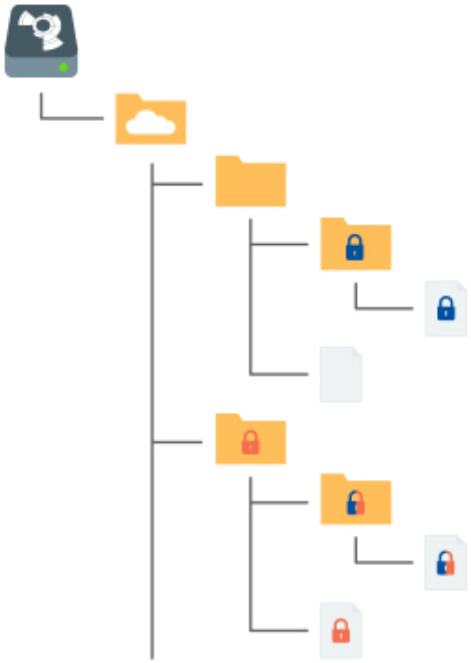
Wir erreichen diese Einfachheit durch die Erstellung eines virtuellen Laufwerks auf Ihrem Computer. Es funktioniert wie ein **zur Verschlüsselung fähiges Fenster zu Ihren Daten**. Auf all Ihre Dateien – unabhängig davon, ob sie verschlüsselt sind oder nicht – kann **über dieses virtuelle Boxcryptor-Laufwerk zugegriffen werden**.

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 fragen, ob Sie das Objekt verschlüsseln möchten oder nicht.

Mit Ihren Dateien arbeiten

Mit Boxcryptor müssen Sie **Dateien nicht manuell entschlüsseln** um damit zu arbeiten. Boxcryptor ist tief in macOS integriert, indem es ein virtuelles Laufwerk erzeugt. 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 das Boxcryptor-Laufwerk 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 klicken Sie mit rechts auf **die Datei oder den Ordner → Boxcryptor → Manage Permissions**. 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. Alle Dateien und Ordner im Boxcryptor Laufwerk sind **mit kleinen Icons markiert**, die ihren aktuellen Status anzeigen.

 **verschlüsselt**

 **nicht verschlüsselt**

Falls Sie Dropbox Smart Sync verwenden (oder eine andere Cloud, die die On-Demand Funktion unterstützt), gibt es zusätzliche Status und Icons:

 **verschlüsselt** und **online-only**

 **verschlüsselt** und der Ordner enthält **sowohl** verschlüsselte als auch nicht verschlüsselte Dateien

 **nicht verschlüsselt** und **online-only**

 **nicht verschlüsselt** und der Ordner enthält **sowohl** verschlüsselte als auch nicht verschlüsselte Dateien

Verschlüsselung vorhandener Dateien und Ordner

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

- Navigieren Sie zu der verschlüsselnden Datei oder dem zu verschlüsselnden Ordner.
- Rechts-Klicken Sie die Auswahl und wähen Sie **Boxcryptor → Verschlüsseln** im Kontextmenü.
- Warten Sie die erfolgreiche Synchronisation Ihres Dienstanbieters ab.

Bitte **warten Sie, bis die Software Ihres Cloud-Anbieters die Dateien vollständig synchronisiert hat**, bevor Sie mit diesen arbeiten. Das hilft, Synchronisationskonflikten vorzubeugen.

Hinweis: Um die Synchronisationsergebnisse zu verbessern, fügt Boxcryptor eine **_encrypted**-Endung an die Namen der verschlüsselten Dateien und Ordner an. Nachdem die Synchronisation beendet wurde, können Sie diese ohne Probleme wieder umbenennen.

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: 恂惊捋抱砻捻殡栟瞻攉獭漢怏搬濂檬狮楻梗扒柜樨賧.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 existierende 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 **Boxcryptor Preferences** → **Security** → **Encryption** und wählen Sie **Enable filename encryption**.

Um die Dateinamenverschlüsselungs-Einstellungen von bereits verschlüsselten Dateien und Ordnern zu verändern, führen Sie einen Rechtsklick auf sie aus und wählen Sie **Boxcryptor** → **Enable / Disable filename encryption** im Kontextmenü. Folgen Sie den Instruktionen und stellen Sie sicher, dass die Dateien fertig synchronisiert sind, bevor Sie mit Ihnen weiterarbeiten.

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: Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie entschlüsseln möchten, und wählen Sie **Boxcryptor** → **Entschlüsseln** .
- Wenn Sie Ihre Dateien im entschlüsselten Modus kopieren oder verschieben möchten: Wählen Sie einfach die Dateien im Boxcryptor-Laufwerk im Windows Explorer aus und kopieren Sie diese an den neuen Speicherort. Die Daten werden automatisch entschlüsselt.

On-Demand-Dateien

Einige Cloud-Anbieter bieten an, nicht alle Dateien automatisch auf Ihr Gerät zu synchronisieren.

Stattdessen wird nur die Verzeichnisstruktur auf dem Gerät abgebildet und Dateien werden nur heruntergeladen, wenn sie geöffnet werden. So werden wertvoller Speicherplatz und Bandbreite gespart, während trotzdem auf alle Dateien vom Computer aus zugegriffen werden kann.

Dropbox Smart Sync

Dropbox Smart Sync kennt drei Zustände für Dateien und Ordner:

- **Nur online verfügbare Inhalte** werden in Ihrem lokalen Dropbox-Ordner angezeigt, belegen aber nicht den Speicherplatz, den Dateien sonst belegen würden. Im Datei-Explorer sehen Sie die Datei, der Inhalt wird jedoch nur dann vollständig heruntergeladen, wenn Sie ihn brauchen. Heruntergeladen werden nur Informationen über die Datei wie zum Beispiel der Name der Datei, der Speicherort und das Datum der Aktualisierung.
- **Gemischte Ordner** enthalten sowohl lokal gespeicherte als auch reine Online-Inhalte.
- **Lokale Inhalte** werden heruntergeladen und auf der Festplatte Ihres Computers gespeichert. Sie können diese Dateien direkt über Anwendungen auf Ihrem Computer bearbeiten.

Boxcryptor bewahrt den Smart-Sync-Status der Dateien in Dropbox, lädt Dateien via Dropbox on-Demand herunter, wenn eine andere Anwendung sie öffnet und zeigt den Smart-Sync-Status im Boxcryptor-Laufwerk an.

Dateien und Ordner sind **mit kleinen Icons markiert**, die ihren aktuellen Status anzeigen.

Anmerkung: Der Smart-Sync-Status von Ordnern wird nur anhand der Dateien im obersten Ordner bestimmt. Dateien in Unterordnern werden aus Performance-Gründen nicht berücksichtigt.

Öffnen von nur online verfügbaren Dateien

Sie können nur online verfügbare Dateien im Boxcryptor-Laufwerk direkt ansteuern und öffnen. Boxcryptor wird sofort einen Download via Dropbox Smart Sync auslösen und warten, bis er abgeschlossen ist. Nach dem Ende des Downloads wird die Datei geöffnet. Falls der Download länger als 3 Sekunden benötigt, wird Boxcryptor das Öffnen der Datei abbrechen, um die Verfügbarkeit des Boxcryptor-Laufwerks zu erhalten. Der Download-Fortschritt wird direkt im Finder angezeigt werden. Sie können erneut versuchen, die Datei zu öffnen, wenn der Download abgeschlossen ist.

Herunterladen von nur online verfügbaren Inhalten

Falls Sie eine nur online verfügbare Datei lokal verfügbar machen möchten, ohne sie öffnen zu müssen, führen Sie einen Rechtsklick auf sie aus und wählen Sie: **Boxcryptor → Download**. Bitte beachten Sie, dass es derzeit nicht möglich ist, diese Operation rückgängig zu machen, also eine lokal verfügbare Datei nur online verfügbar zu machen, oder, aufgrund von Beschränkungen durch Dropbox, einen ganzen Ordner herunterzuladen (nur einzelne Dateien möglich). Falls Sie dies tun möchten, verwenden Sie bitte die Dropbox-App. Sie können die Originaldatei im Dropbox-Ordner direkt markieren, indem Sie in Boxcryptor auf sie rechtsklicken und **Boxcryptor → Show Original in Dropbox** wählen.

Kann ich die Berechtigungen von nur online verfügbaren Ordnern bearbeiten?

Berechtigungen werden in einer Datei namens FolderKey.bch in einem Ordner gespeichert. Wenn diese Datei nur online verfügbar ist, wird sie automatisch von Dropbox heruntergeladen, wenn Sie die Rechteverwaltung in Boxcryptor öffnen. Falls die Datei nicht heruntergeladen werden kann, weil zu dem Zeitpunkt keine Internetverbindung besteht, können die Berechtigungen zu diesem Zeitpunkt nicht geändert werden. In diesem Fall stellen Sie eine Verbindung her und versuchen Sie es erneut.

Wieso kann das Öffnen einer Office-Anwendung (Word, Excel, Powerpoint) sehr langsam sein?

Wenn Sie eine Office-Anwendung öffnen, versucht sie, alle kürzlich geöffneten Dateien zu öffnen. Falls diese Dateien nur online verfügbar sind, lädt Dropbox sie herunter und blockiert die öffnende Anwendung, bis der Download abgeschlossen ist. Die Liste der kürzlich verwendeten Dateien in der Office-Anwendung zu leeren, löst dieses Problem.

Wieso sind manche Dateien immer lokal, sogar wenn ich sie nur online verfügbar gemacht habe?

Infos hierzu bietet die Frage zuvor. Wenn eine Datei in der Liste der kürzlich geöffneten Dateien einer Office-Anwendung vorhanden ist, wird das Öffnen dieser Anwendung dazu führen, dass Dropbox sie herunterlädt. Die Liste der kürzlich verwendeten Dateien in der Office-Anwendung zu leeren, löst dieses Problem.

Wann brauche ich eine Internet-Verbindung, wenn ich mit eingeschaltetem Smart Sync arbeite?

Sie brauchen eine Internetverbindung, wenn Sie versuchen, eine nur online verfügbare Datei zu öffnen, oder wenn Sie in einem verschlüsselten Ordner arbeiten, dessen Ordner-Schlüssel-Datei (FolderKey.bch) nur online verfügbar ist. Wir empfehlen, verschlüsselte Ordner immer vollständig lokal oder nur online verfügbar zu machen und gemischte Ordner zu vermeiden, wenn Sie mit einer schlechten Internetverbindung rechnen müssen.

Kann ich eine Datei oder einen Ordner im Boxcryptor-Laufwerk nur online verfügbar machen?

Nein, es ist derzeit nicht möglich, eine Datei oder einen Ordner nur online verfügbar zu machen, wenn Sie sich im Boxcryptor-Laufwerk befinden. Falls Sie eine Datei oder einen Ordner nur online verfügbar machen möchten, müssen Sie dies direkt im Dropbox-Ordner tun. Wählen Sie **Smart Sync → nur online verfügbar** im Dropbox-Kontextmenü. Um eine Datei oder einen Ordner im Dropbox-Ordner zu finden, können Sie im Boxcryptor-Laufwerk auf sie rechtsklicken und wählen: **Boxcryptor → Show Original** in Dropbox.

Kann ich einen Ordner im Dropbox-Verzeichnis herunterladen?

Nein, es ist derzeit nicht möglich, einen Ordner herunterzuladen und ihn lokal verfügbar zu machen, wenn Sie sich im Boxcryptor-Laufwerk befinden. Falls Sie einen Ordner lokal verfügbar machen möchten, müssen Sie Falls Sie dies tun möchten, verwenden Sie bitte die Dropbox app und wählen Sie **Smart Sync → Lokal** im Dropbox-Kontextmenü. Sie können die Originaldatei im Dropbox-Ordner direkt markieren, indem Sie in Boxcryptor auf sie rechtsklicken und **Boxcryptor → Show Original in Dropbox** wählen.

Kann ich Spotlight verwenden, um nur online verfügbare Dateien zu finden?

Sie können nur online verfügbare Dateien anhand ihres Namens finden, aber es ist nicht möglich, sie anhand ihres Inhalts zu finden, denn vor dem Download enthalten diese Dateien noch keinen Inhalt.

Google Drive File Stream

Google Drive File Stream wird offiziell von Boxcryptor auf allen Plattformen unterstützt. Alle Information dazu finden Sie auf unserem Blog.

Box Drive

Box Drive wird ebenfalls offiziell von Boxcryptor unterstützt.

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

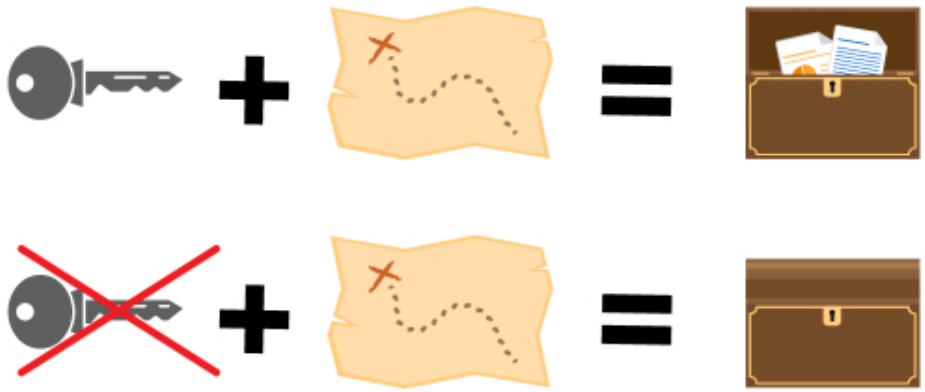
Um zu verstehen, wie das Teilen von verschlüsselten Datein funktioniert, ist es hilfreich zu wissen, wie Programme unverschlüsselte und verschlüsselte Datein behandeln.

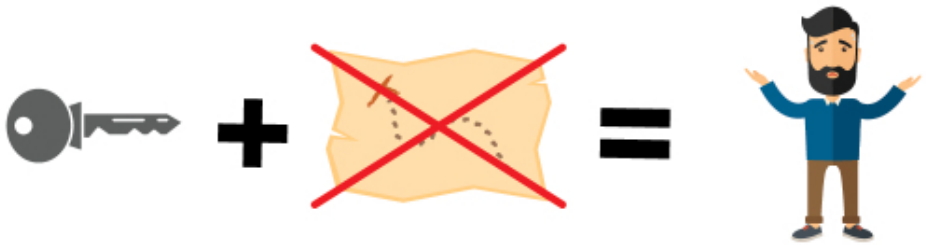
Wenn Sie eine unverschlüsselte Datei auf Ihrem Gerät oder in der Cloud speichern, speichert das von Ihnen gewählte Programm die Datei und die darin enthaltenen Informationen. Diese Datei kann dann von jedermann, der physischen Zugang hat, gelesen oder verändert werden. Wenn Sie eine Datei jedoch verschlüsseln, 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:

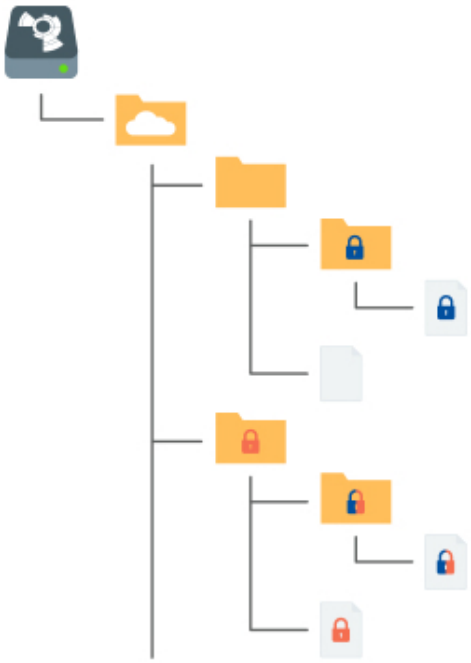
1. Teilen Sie die Datei physisch bei Ihrem Cloud-Anbieter. Bitte lesen Sie in der Dokumentation Ihres Anbieters nach, wie Dateien oder Verzeichnisse geteilt werden können.
2. Teilen Sie den kryptographischen Schlüssel in Boxcryptor. Boxcryptor verwendet für jede Datei einen Schlüssel. Der Schlüssel wird 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:

- Rechtsklick auf **Datei oder Ordner** → **Boxcryptor** → **Manage Permissions**.
- 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.
- Erneut Rechtsklick auf **Datei oder Ordner** → **Boxcryptor** → **Show Original at Provider**.
- Rechtsklick auf den Ordner → **Share**.

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. Die Gruppenverwaltung ist innerhalb des Kontos verfügbar, indem Sie sich auf unserer Website anmelden.

Unumkehrbare Operationen wie **rename**, **delete** oder **grant** und **revoke ownership** kann nur der Eigentümer der Gruppe (**owner**) vornehmen. Sie können andere Mitglieder als Eigentümer festlegen und ihnen die Eigentumsrechte 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 Synchronisation nicht notwendig.

Einstellungen

App-Schutz

Der App-Schutz verhindert **unbefugten Zugriff** auf Boxcryptor.

Wenn diese Funktion aktiviert ist, können Sie **verschiedene Authentifizierungsmethoden** festlegen. Sie müssen sich dann mit einer festgelegten Methode für die Nutzung von Boxcryptor authentifizieren.

Sie können maximal fünfmal eine ungültige Authentifizierung eingeben. Wenn Ihre Authentifizierung fehlschlägt, müssen Sie Ihr Boxcryptor-Passwort eingeben oder Boxcryptor auf die Werkseinstellungen zurücksetzen.

Aus diesen Authentifizierungsmethoden können Sie wählen:

- **vierstelliger PIN-Code**: Wenn festgelegt, müssen Sie einen vierstelligen PIN Code eingeben.
- **Passwort**: Wenn festgelegt, müssen Sie Ihr Boxcryptor-Passwort eingeben.- **Touch ID and Geräte-Passwort**: Ist dies aktiviert, muss der Benutzer seinen Fingeradruck unter Verwendung des Fingerabdruck-Sensors am Gerät einlesen. Diese Funktion ist nur bei Geräten verfügbar, die Touch ID unterstützen. Falls Sie das bevorzugen, stellt Apple eine Ersatzfunktion für Touch ID zur Verfügung, die eine Eingabe des Geräte-Passworts, statt Touch ID, ermöglicht.

Boxcryptor erfordert beim Starten eine Authentifizierung. Anschließend läuft Boxcryptor, bis Sie die Software gezielt beenden. Falls Sie Boxcryptor für die Zeit absichern wollen, in der Sie sich nicht an Ihrem Gerät befinden, benutzen Sie bitte die Funktionen des Betriebssystems, um das Gerät manuell oder automatisch nach einer bestimmten Zeit zu sperren.

Sie können die Sicherheits-Funktionen in den Einstellungen aktivieren: **Boxcryptor-Menüleisten-Symbol → Preferences → Security**.

Anmerkung: Falls es einem Hacker gelingt, Zugriff auf Ihr Betriebssystem zu erlangen, ist es ihm theoretisch möglich die lokal gespeicherten Boxcryptor-Einstellungen zu verändern und die Sicherheits-Funktionen zu umgehen. Während die Funktion Ihnen einen verbesserten Schutz Ihrer verschlüsselten Daten auf Ihrem Computer bieten kann, garantiert sie keine 100%ige Sicherheit gegen erfahrene Angreifer mit Zugriff auf Ihr Betriebssystem. Wie empfehlen den Best Practices für die lokale Sicherheit Ihrer Geräte zu folgen, um eine solche Situation zu vermeiden.

Boxcryptor-Einstellungen

Um die Boxcryptor-Einstellungen aufzurufen, klicken Sie auf das Boxcryptor-Icon in der Menüleiste und wählen Sie **Einstellungen**. Navigieren Sie zu zum **Erweitert**- oder **Updates**-Tab, um die Autostart- oder Update-Einstellungen zu verändern.

Die Standardeinstellungen sind:

- Automatische Prüfung auf Updates ("Automatically check for updates")
- Automatisches Senden von Diagnostik- und Nutzungsdaten ("Automatically send Diagnostic and Usage Data")

Außerdem können Sie die folgenden Boxcryptor-Einstellungen verändern:

> ⚠ Eine Änderung dieser Einstellungen könnte zu unerwünschtem Verhalten von Boxcryptor führen. Bitte führen Sie **keine** Änderungen durch, es sei denn, Sie sind ein **erfahrener Nutzer**.

- **Mount for all users**: System Accounts können auf Boxcryptor zugreifen.
- **Mount as fixed disk**: Obwohl das Boxcryptor-Laufwerk ein virtuelles Laufwerk ist, wird diese Option dazu führen, dass es aussieht und behandelt wird wie ein physisches Laufwerk.
- **Enable trash**: Das Löschen von Dateien wird sie in den Papierkorb verschieben, so dass sie wiederhergestellt werden können, falls nötig.
- **Enable Spotlight**: Erlaubt Spotlight, Dateien in Boxcryptor zu indizieren und zu finden.

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.

Zurück zu einem Online-Boxcryptor-Konto wechseln

Wenn Sie zunächst mit einem lokalen Konto begonnen hatten, aber nun von allen Vorteilen eines vollständigen Boxcryptor-Kontos profitieren möchten, können Sie Ihr lokales Konto hier in ein reguläres Boxcryptor-Konto umwandeln.

Dies funktioniert nur, wenn Sie noch kein Online-Boxcryptor-Konto haben.

Wenn Sie vorübergehend ein lokales Konto mit Ihren exportierten Schlüsseln verwenden und zurückwechseln möchten, können Sie sich einfach von Boxcryptor **abmelden** und sich wieder mit Ihrem Online-Konto anmelden. Sofern Sie **keine Kontozurücksetzung** durchgeführt haben, sind Ihre Dateien weiterhin zugänglich.

Eine Schlüsseldatei exportieren

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

Eine bestehende Schlüsseldatei öffnen

1. Klicken Sie im Anmeldebildschirm auf •••.
2. Wählen Sie **Lokales Konto**.
3. Klicken Sie auf **Lokales Konto nutzen**.
4. Ziehen Sie Ihre Schlüsseldatei in das graue Feld.
5. Melden Sie sich mit Ihrem Passwort bei Boxcryptor 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.

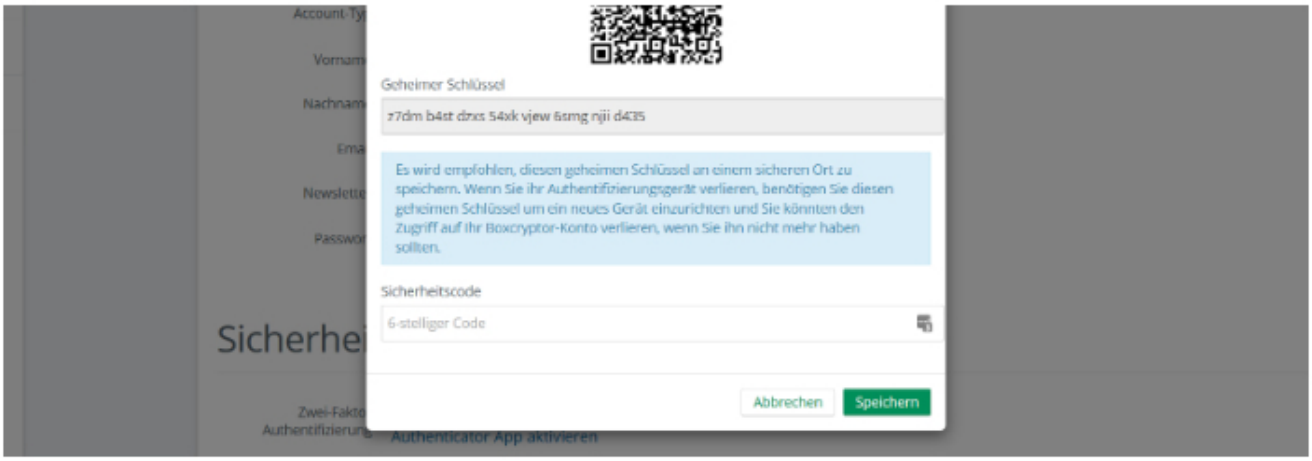
Authenticator-App

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-Sperre

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 die App-Sperre 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

Neue Boxcryptor für macOS Beta

Which macOS versions are supported?

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

Which Macs are supported?

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

Where can I get the Beta?

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

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

Are special instructions required for the installation?

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

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

1. Reboot your Mac into Recovery Mode
2. Open Utilities -> Startup Security Utility
3. Select and unlock your system volume and click Security Policy...
4. Choose Full Security
5. Restart your Mac

Can I use the Beta for production data?

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

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

Where are files encrypted?

As you expect from Boxcryptor files stored in the cloud are always encrypted and encryption is performed locally on your Mac all the time. Only encrypted files leave your device.

However, in contrast to Boxcryptor for macOS in the past, **files stored locally on your Mac are not encrypted by Boxcryptor anymore due to technical limitations by Apple's File Provider platform.** File Provider apps must store files in cleartext on the local filesystem so that their content can get picked up by macOS and presented to the user. This affects file contents and file names.

Here's the encryption state by location:

- **In the cloud:** Files are always protected by Boxcryptor's encryption
- **On your Mac with FileVault:** Files are protected by FileVault's encryption
- **On your Mac without FileVault:** Files are not protected (not recommended)

We strongly recommend the use of local full-disk encryption for every Mac – regardless if you are using a previous version of Boxcryptor for macOS or the new Boxcryptor for macOS Beta or even if you don't use Boxcryptor at all. Full-disk encryption is an integral part of local device security and can easily be achieved by turning on FileVault on any Mac.

> By using FileVault, files available in the new Boxcryptor for macOS Beta are still protected by FileVault's encryption on the local disk despite appearing as cleartext when your Mac is in use. Learn more about FileVault here: https://support.apple.com/en-us/HT204837

Where can I find Boxcryptor on my Mac?

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

As every File Provider app, Boxcryptor is now available in `~/Library/CloudStorage` where a sync folder for each connected cloud provider is created. **These folders are also accessible in the Finder's Location section.**

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

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

Why is everything new?

A main driver for the new Boxcryptor for macOS version is Apple's strategy to disallow third party kernel extensions in macOS in order to further secure and close down the Mac operating system. Apple started to deprecate third party kernel extensions a few years ago and successively made it more difficult to use them. While a kernel extension could be loaded "on-the-fly" in the past, macOS 10.15 Catalina started to require a system reboot during the loading process.

Nowadays, Macs with Apple Silicon processors additionally require the modification of the Mac's Security Policy in Recovery Mode to allow third party kernel extension loading. All signs indicate that third party kernel extensions will not work at all in future versions of macOS. Holding on to our existing concept using a virtual Boxcryptor drive based on a kernel extension would not be sustainable anymore.

Due to Apple's decisions, we have been forced to come up with a new concept how Boxcryptor for macOS works in the years to come. At the same time, we are excited about the new possibilites and experiences this new integration into macOS opens up for Boxcryptor in the future.

Can I use Spotlight again?

Yes, finally! A major advantage of the new File Provider-API over the old virtual drive is that Spotlight works out-of-the-box without requiring special handling by Boxcryptor. This means that **Spotlight indexes files and folders in Boxcryptor locations automatically and by default.** Spotlight support is not an optional advanced setting anymore, but a first-class default experience for every user.

Spotlight indexes file and folder metadata of all items in Boxcryptor locations. File contents are only searchable for downloaded files which are locally available for indexing due to technical limitations.

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

Which limitations are known?

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

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

- Managing permissions is not yet supported

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

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

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

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

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

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

Wie erstellt man ein Debug-Log?

Wenn Sie auf ein Problem stoßen, kann ein Debug-Log sehr hilfreiche Einblicke liefern, um es zu beheben. Sie können ein Log erstellen, indem Sie die folgenden Schritte ausführen:

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** und senden Sie sie uns an support@boxcryptor.com

Bitte beachten Sie, dass die Protokolle Metainformationen über Ihre Datei- und Ordnerstruktur enthalten, einschließlich Tags, Dateinamen, Dateigrößen usw. Sie enthalten jedoch keine Dateiinhalte.

Boxcryptor erzeugt eine hohe CPU-Last

Die CPU-Last hängt direkt mit der Aktivität im Boxcryptor-Laufwerk zusammen. Wenn viele

Operationen auf dem Boxcryptor-Laufwerk stattfinden – beispielsweise Lesen oder Schreiben von Dateien – steigt die CPU-Last. Finden keine Aktivitäten im Boxcryptor-Laufwerk statt, sollte die CPU-Last gering sein.

Es ist jedoch **möglich, dass diese Aktivitäten nicht sichtbar sind**, zum Beispiel wenn Applikationen Hintergrundaktivitäten ohne direkten Einfluss des Nutzers durchführen. Ein klassisches Beispiel hierzu sind Indexierungen durch Spotlight.

Boxcryptor ist langsam

Eine App ist langsamer als gewöhnlich bei der Nutzung mit Boxcryptor

Falls eine App langsamer als gewöhnlich ist, wenn sie in Verbindung mit Boxcryptor verwendet wird, könnte sie Probleme haben, mit Boxcryptors Verschlüsselung umzugehen. Boxcryptor funktioniert wie ein Filter, der Lese- und Schreib-Anfragen vom Betriebssystem annimmt und sie auf dem Weg verschlüsselt.

Gut entwickelte Apps schreiben ihre Dateien Blöcken. In diesem Fall muss Boxcryptor nur wenige Male aktiv werden und die Leistung wird nicht beeinträchtigt. Manche Apps schreiben allerdings jedes Byte einzeln. Das führt zu vielen Boxcryptor-Aufrufen und verringerter Leistung.

Falls Sie Schwierigkeiten mit einer Ihrer häufig verwendeten Apps haben und Geschwindigkeit Ihnen wichtig ist, könnten Sie einen Alternative ausprobieren, die mit Boxcryptors Verschlüsselung vielleicht besser zurechtkommt.

Ein Hintergrundprozess verursacht hohe Last

Eine langsame Geschwindigkeit des Boxcryptor-Laufwerks kann durch einen Hintergrundprozess verursacht werden, der eine hohe Anzahl an Dateioperationen im Boxcryptor-Laufwerk ausführt ohne dass der Nutzer dies merkt. Da Boxcryptor dann damit beschäftigt ist, all die Dateioperationen des Hintergrundprozesses zu bearbeiten, bleibt weniger Zeit um die Dateioperationen anderer Programme zu bearbeiten. Das Boxcryptor-Laufwerk fühlt sich dann langsam an. Ein klassisches Beispiel hierzu ist ein Dienst zur Erstellung eines Suchindexes, wie z.B. Spotlight.

Inkompatibilitäten mit Anti-Virus Programmen

Das Echtzeit-Scan Feature von Anti-Virus Programmen schaltet sich zwischen Dateioperationen und überprüft diese auf Malware-Verhalten. Dies kann zu Inkompatibilitätsproblemen mit dem virtuellen Boxcryptor-Laufwerk führen wenn das Anti-Virus Programm sowohl Dateioperationen im Boxcryptor-Laufwerk als auch Dateioperationen von Boxcryptor selbst unterbricht. Dies kann zu spürbaren Geschwindigkeitsproblemen oder sogar zu einem Einfrieren des Boxcryptor-Laufwerks führen.

Falls Sie Probleme mit dem Boxcryptor-Laufwerk oder dessen Performance haben und ein Anti-Virus Programm auf Ihrem Mac verwenden, deaktivieren Sie das Echtzeit-Scan Feature oder schließen Sie das Boxcryptor-Laufwerk davon aus, falls dies möglich ist. Sie können zudem den Support Ihres Anti-Virus Programms kontaktieren und auf diese Inkompatibilität hinweisen so dass diese behoben werden kann.

Symbole oder das Kontextmenü werden nicht angezeigt

Mit macOS 10.10 Yosemite hat Apple die neuen App Extensions eingeführt, um erweiterte Funktionalitäten – beispielsweise in Finder – bereitzustellen. Seit Version 2.3.401 (733) von Boxcryptor für macOS ist die Integration von Boxcryptor im Finder, wie von Apple empfohlen, als eine Finder-Sync-Erweiterung implementiert. Die Finder-Integration beinhaltet das Boxcryptor-Kontextmenü, das beim Rechtsklick auf eine Datei oder ein Verzeichnis verfügbar ist, und überlagerte Symbole, die den Verschlüsselungs-Status von Dateien und Verzeichnissen in Boxcryptor wiederspiegeln.

Leider entspricht die Zuverlässigkeit der Finder-Erweiterungen im Allgemeinen nicht immer den Erwartungen und es kann vorkommen, dass die Finder-Integration aus unerfindlichen Gründen fehlt. Wir können dies nicht beeinflussen und nur Apple kann dies beheben. In diesem Artikel werden wir einige Schritte beschreiben, die Sie probieren können, falls Sie von diesem Problem betroffen sind.

Bevor wir uns das Problem genauer ansehen, empfehlen wir Ihnen die folgenden Schritte auszuführen, die Ihr Problem möglicherweise beheben:

- **Neustart von Finder**: Halten Sie die Option-Taste gedrückt und machen Sie einen Rechtsklick auf das Finder-Symbol, um auf „Neu starten" zu klicken
- **Starten Sie Ihren Mac neu**: Klicken Sie auf das Apple-Symbol in der Menüzeile und wählen Sie „Neustart"
- **Boxcryptor neu installieren**: Stoppen Sie Boxcryptor, falls es läuft. Laden Sie die aktuelle Version von Boxcryptor für macOS herunter. Öffnen Sie das Boxcryptor-Installationsprogramm und kopieren Sie die Boxcryptor-App in Ihr Programme-Verzeichnis.

Sollte die Finder-Integration weiterhin fehlen, gehen Sie zu **Systemeinstellungen → Erweiterungen** und prüfen Sie, dass Boxcryptor bei Ihren Finder-Erweiterungen aufgeführt ist. Sollte die Boxcryptor-Finder-Erweiterung nicht aufgeführt sein, könnte ein allgemeines Problem mit Finder-Erweiterungen auf Ihrem Mac der Grund sein. Ein deutlicher Hinweis darauf is ebenso, falls überhaupt keine (Finder)-Erweiterungen aufgeführt werden und auch Dropbox oder andere Erweiterungen fehlen. Der beste Rat in diesem Fall ist, den Apple-Support zu kontaktieren.

Wenn Sie den Fehler selbst suchen wollen sind hier einige Dinge, die Sie ausprobieren können:

Die Boxcryptor-Finder-Erweiterung manuell hinzufügen

Normalerweise sollte macOS die Boxcryptor-Finder-Erweiterung automatisch erkennen, sobald Boxcryptor zum ersten Mal gestartet wird. In seltenen Fällen ist dies nicht der Fall und die Erweiterung wird nicht automatisch geladen. Um dies zu beheben, können Sie versuchen die Erweiterung mit folgenden Schritten manuell hinzuzufügen:

1. Öffnen Sie die **Terminal**-Applikation.
2. Führen Sie das folgende Kommando aus: `pluginkit -a /Applications/Boxcryptor.app/Contents/PlugIns/Rednif.appex`

Temporär die System-Integrity-Protection ausschalten

System-Integrity-Protection (SIP) ist ein essentieller und wichtiger, neuer Sicherheitsmechanismus, der mit macOS 10.11 El Capitan eingeführt wurde, um zu verhindern, dass Malware in Ihrem Betriebssystem herumpfuscht. Leider scheint SIP gelegentlich auch das Erweiterungs-System von macOS zu stören und wir haben Berichte gesehen, in denen die temporäre Abschaltung von SIP dazu führte, dass Erweiterungen wieder geladen werden konnten und auch nach Wiedereinschalten von SIP noch funktionierten. Sie sollten wirklich vorsichtig beim Ändern von SIP sein und sich der Konsequenzen Ihrer Handlung bewusst sein. Informationen zu SIP finden Sie hier und hier.

Wie schalte ich System Integrity Protection aus?

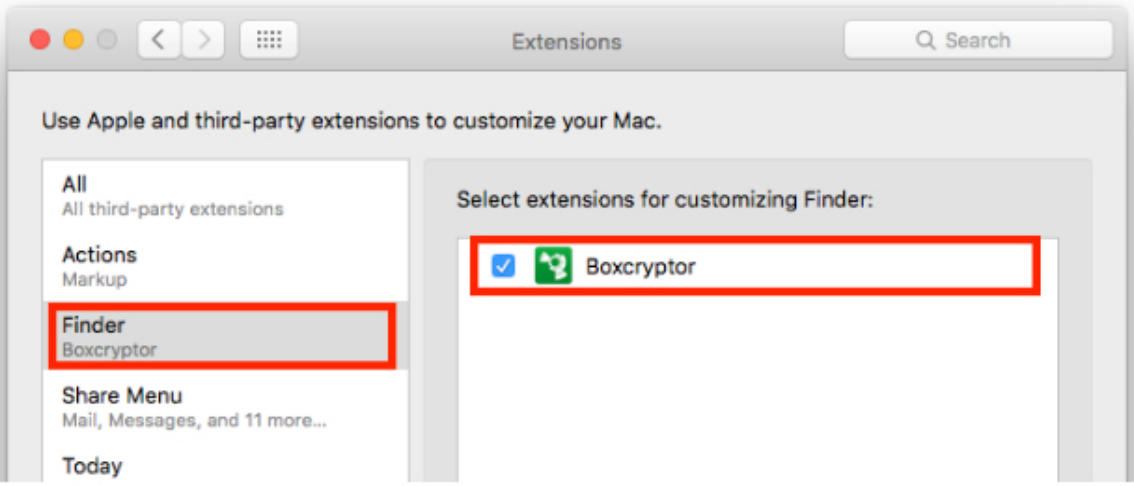
Achtung: Wie empfehlen im Allgemeinen keinerlei Systemsicherheits-Mechanismen auszuschalten. Führen Sie diese Schritte nur aus, wenn Sie wissen was Sie tun und tun Sie dies nur auf eigene Verantwortung.

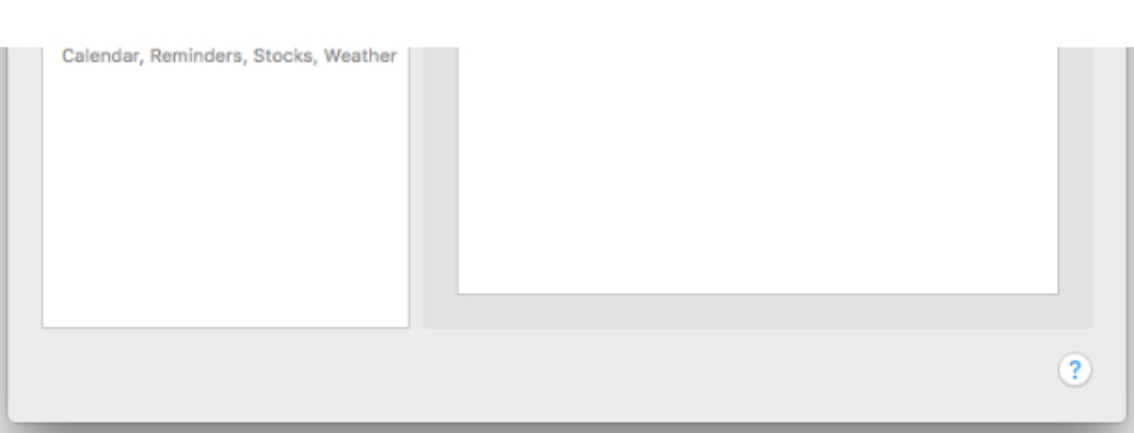
1. Starten Sie Ihren Mac neu und halten Sie **Cmd+R** gleichzeitig gedrückt, um in den **Recovery Mode** zu booten.
2. Im macOS-Utilities-Bildschirm öffnen Sie **Utilities** und klicken auf **Terminal**.
3. Finden Sie den aktuellen Status von SIP durch Eingabe des folgenden Kommandos heraus: `csrutil status`.
4. Schalten Sie SIP durch Eingabe des folgenden Kommandos aus: `csrutil disable`.
5. Starten Sie Ihren Mac neu und prüfen Sie, dass Erweiterungen geladen wurden.
6. Starten Sie Ihren Mac erneut im Recovery Mode, öffnen Sie Terminal und schalten Sie SOP wieder durch Eingabe des folgenden Kommandos ein: `csrutil enable`.

Neuinstallation von macOS

Wir haben Berichte gesehen, in denen eine Neuinstallation von macOS das Problem löst und Erweiterungen wieder erfolgreich geladen werden, nachdem das Betriebssystem frisch aufgesetzt wurde. Speziell wenn Erweiterungen generell fehlen (zum Beispiel die Dropbox-Erweiterung, obwohl sie installiert ist), kann eine Neuinstallation von macOS eventuell die einzige Lösung sein, damit das Erweiterungs-Teilsystem wieder richtig arbeitet.

Stellen Sie sicher, dass die Boxcryptor-Finder-Erweiterung aktiviert ist





Falls die Boxcryptor-Finder-Erweiterung geladen und in der Liste unter **Systemeinstellungen → Erweiterungen** aufgeführt ist, prüfen Sie, dass diese auch aktiviert ist und dass das Kontollkästchen angehakt ist.

Vermeiden Sie Konflikte von Erweiterungen

Zu jedem Zeitpunkt darf lediglich **eine** Erweiterung für ein bestimmtes Verzeichnis aktiv sein, unabhängig davon, wie viele Erweiterungen aktiviert sind. Falls zwei Erweiterungen für das gleiche Verzeichnis registriert sind, wird nur eine davon in Finder verfügbar sein und die andere wird, abhängig davon welche Erweiterung macOS zuerst geladen hat, ignoriert.

Versuchen Sie andere Erweiterungen zu deaktivieren um mögliche Konflikte zu finden. Wir haben Berichte gesehen, wo speziell die Google Drive und Finder-Erweiterung der Synology-Cloud-Station Probleme mit anderen Erweiterungen verursacht haben.

> Falls keiner dieser Tipps hilft und die Boxcryptor-Finder-Erweiterung nach wie vor nicht auf Ihrem Mac funktioniert, können wir Ihnen eventuell helfen, wenn Sie uns direkt kontaktieren. Aber Sie können sich sicher sein, dass Sie nicht alleine sind und wir hoffen, dass Apple die Erweiterungen in Zukunft reparieren wird.

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 kann ich ein Debug Log erstellen?

Haben Sie Probleme mit der neuesten **Boxcryptor für macOS Beta**? Anweisungen zum Erstellen eines Debug Logs finden Sie hier (unter **Wie erstellt man ein Debug-Log?**)

- Beenden Sie Boxcryptor.
- Öffnen Sie die **Terminal** App und führen Sie den folgenden Befehl aus:
  `/Applications/Boxcryptor.app/Contents/MacOS/Boxcryptor --debug`
- Wiederholen Sie alle Schritte, die zu der unerwarteten Reaktion des Programs geführt haben.
- Beenden Sie Boxcryptor, indem Sie in der Menüleiste auf → **Quit Boxcryptor** klicken.

Ein Debug Log (`Boxcryptor-<Timestamp>.rawnsloggerdata`) wird erstellt und in **~/Library/Logs/Boxcryptor** abgespeichert.

Wie kann ich auf das Log-Verzeichnis zugreifen?

- Öffnen Sie **Finder** und wählen sie **Go → Go to Folder... (Cmd+Shift+G)**.
- Tippen Sie `~/Library/Logs/Boxcryptor` und klicken dann auf go.

Was mache ich mit meinem Debug Log?

Verwenden Sie unser Boxcryptor Hilfe Formular, um uns die Datei mit einer genauen Fehlerbeschreibung zu senden, oder schreiben Sie unserem Support-Team und fügen Sie das Debug Log bei.

Da Debug Logs sehr schnell sehr umfangreich werden können, empfehlen wir, die Debug-Log-Datei zu komprimieren, um die Dateigröße vor dem Versenden zu reduzieren.

Zusätzliche Systeminformationen

Wenn ihre Systemkonfiguration von Bedeutung ist, können sie Informationen darüber folgendermaßen exportieren:

1. Öffnen Sie **Spotlight** → schreiben Sie `System Information` → drücken Sie **Enter**. Nun öffnet sich die Systeminformations-Übersicht.
2. Gehen Sie nun in der Menüleiste auf `Datei` → `speichern`, um die Informationen zu exportieren und uns zusätzlich zukommen zu lassen.

Dateisystemzugriffe bereits vor Ausführung loggen

In seltenen Fällen kann es von Interesse sein, Zugriffe auf das Boxcryptor Laufwerk bereits vor der Ausführung der Dateioperation zu protokollieren. Sie erfahren hier (unter **eager logging**), wie Sie diese Funktion aktivieren können.

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:

Fehlermeldung: Es scheint keine Internetverbindung zu bestehen

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: Das 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 offline weiterarbeiten. Alle Dateien bleiben verfügbar. Sie können jedoch keine Boxcryptor-Rechte verändern oder andere Online-Funktionen von Boxcryptor nutzen.

Wie deinstalliere ich Boxcryptor?

Da Boxcryptor tief in macOS integriert ist und der Mac keinen eigenen Deinstallations-Mechanismus bereitstellt, folgen Sie bitte diesem Leitfaden, um Boxcryptor vollständig vom System zu entfernen.

1. Beenden Sie Boxcryptor.
2. Öffnen Sie **Systemeinstellungen** → **Erweiterungen** → **Finder** und deaktivieren Sie Boxcryptor.
3. Löschen 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 Einträge, die mit *com.boxcryptor.osx.* beginnen.
6. Verschieben Sie **Boxcryptor.app** in den Papierkorb.

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

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.

Erweiterte Client-Konfiguration

Einige Einstellungen von Boxcryptor werden in der Benutzeroberfläche nicht angezeigt. Obwohl es im Allgemeinen nicht empfohlen wird, diese Einstellungen zu ändern, können erfahrene Benutzer oder Administratoren dadurch Boxcryptor besser an ihre Bedürfnisse anzupassen.

> ⚠ Die versteckten Einstellungen werden geladen, wenn Boxcryptor gestartet wird. Falls Boxcryptor ausgeführt wird, während Sie eine versteckte Einstellung ändern, müssen Sie Boxcryptor neu starten, damit die Änderung angewendet wird. Beachten Sie auch, dass bei dem Schlüssel zwischen Groß- und Kleinschreibung unterschieden wird.

Versteckte Einstellungen verwalten

Versteckte Einstellungen werden im macOS-Benutzerstandardeinstelluneg gespeichert und können mit dem Befehl **defaults** via Terminal verwaltet werden. Die Benutzerstandardeinstellungen von Boxcryptor für macOS werden in der Domäne "com.boxcryptor.osx" gespeichert. Um die versteckten Einstellungen zu verwalten, können Sie die folgenden Befehle in Terminal ausführen. Bitte lesen Sie die Manpages für den Befehl **defaults**, um mehr über die Verwendung zu erfahren.

- **defaults read com.boxcryptor.osx KEY** Liest den aktuellen Wert von KEY
- **defaults write com.boxcryptor.osx KEY VALUE** Speichert VALUE von KEY
- **defaults remove com.boxcryptor.osx KEY** Löscht KEY

Liste der versteckten Einstellungen

- **autoDetectRemovableDrives** Standardmäßig erkennt Boxcryptor Wechseldatenträger automatisch und fügt sie automatisch als Speicherorte hinzu. Setzen Sie diesen Wert auf "NO", um die automatische Erkennung von Wechseldatenträgern zu deaktivieren. Standard: YES
- **disableAccessControlLists** Standardmäßig unterstützt Boxcryptor Zugriffssteuerungslisten (ACLs). Setzen Sie diesen Wert auf "YES", um diese Unterstützung zu deaktivieren, wenn Sie sie nicht benötigen. Da das Abrufen von ACLs zusätzliche Dateivorgänge erfordert, kann das Deaktivieren der Unterstützung für ACLs die Leistung von Boxcryptor geringfügig verbessern. Standard: NO

- **disableAliases** Standardmäßig erstellt Boxcryptor Aliase für das Boxcryptor-Laufwerk in der Finder-Seitenleiste und auf dem Desktop, wenn Finder dies nicht anders anzeigt. Setzen Sie diesen Wert auf "YES", um die Erstellung von Aliasen durch Boxcryptor zu deaktivieren. Standard: NO
- **disableDesktopAlias** Standardmäßig erstellt Boxcryptor einen Alias für das Boxcryptor-Laufwerk auf dem Desktop, wenn der Finder ihn sonst nicht anzeigt. Setzen Sie diesen Wert auf "YES", um die Erstellung des Desktop-Alias durch Boxcryptor zu deaktivieren. Hinweis: Boxcryptor erstellt den Alias nur, wenn im Finder keine verbundenen Server angezeigt werden (das Boxcryptor-Laufwerk ist dann als Remote-Festplatte bereitgestellt). Bitte deaktivieren Sie in diesem Fall Finder -> Einstellungen -> Allgemein -> Verbundene Server. Standard: NO
- **disableSidebarAlias** Standardmäßig erstellt Boxcryptor einen Alias für das Boxcryptor-Laufwerk in der Finder-Seitenleiste, wenn der Finder ihn sonst nicht anzeigt. Setzen Sie diesen Wert auf "YES", um die Erstellung des Finder-Seitenleisten-Alias durch Boxcryptor zu deaktivieren. Standard: NO
- **disablePlainTextWarning** Standardmäßig fragt Boxcryptor, ob Sie eine Datei oder einen Ordner verschlüsseln möchten, wenn Sie sie in einem Klartextordner erstellen/kopieren/verschieben. Sie können dieses Verhalten deaktivieren, indem Sie diesen Wert auf "YES" setzen. Boxcryptor erstellt dann immer Klartextdateien/Ordner in Klartextordnern und fordert keine Verschlüsselung an. Wichtig: In diesem Fall werden nur Dateien oder Ordner verschlüsselt, die in bereits verschlüsselte Ordner erstellt/kopiert/verschoben wurden. Standard: NO
- **hidePlaintextFilesFromSpotlight** Standardmäßig werden alle Dateien und Ordner auf dem Boxcryptor-Laufwerk von Spotlight indiziert, wenn diese aktiviert ist. Wenn Sie diesen Wert auf "YES" setzen, zeigt und indiziert Spotlight nur verschlüsselte Dateien und ignoriert alle Klartextdateien auf dem Boxcryptor-Laufwerk. Standard: NO
- **revertFileModificationDateOnPermissionChange** Beim Ändern der Berechtigungen für verschlüsselte Dateien oder Ordner fügt Boxcryptor dem Änderungsdatum einige Sekunden hinzu, damit Synchronisierungs-Apps diese Änderung besser erkennen und synchronisieren können. Wenn sich das Änderungsdatum beim Ändern von Berechtigungen in Boxcryptor nicht ändern soll, können Sie diesen Wert auf "YES" setzen. Boxcryptor setzt dann das Änderungsdatum auf den ursprünglichen Wert zurück, nachdem die neuen Berechtigungen angewendet wurden. Standard: NO
- **eagerLogging** Wenn die Protokollierung aktiviert ist, protokolliert Boxcryptor standardmäßig Dateisystemereignisse, nachdem sie auf dem virtuellen Boxcryptor-Laufwerk ausgeführt wurden. Wenn Sie diesen Wert auf "YES" setzen, protokolliert Boxcryptor auch das Dateisystemereignis *vor* der Ausführung.

Beispiele

- **defaults write com.boxcryptor.osx disableAliases -bool YES** Deaktiviert die automatische Erstellung von Finder-Seitenleisten- und Desktop-Aliasen für das Boxcryptor-Lauwerk.
- **defaults remove com.boxcryptor.osx disableAliases** Stellt das Standardverhalten von Boxcryptor bezüglich der Aliaserstellung wieder her.

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.

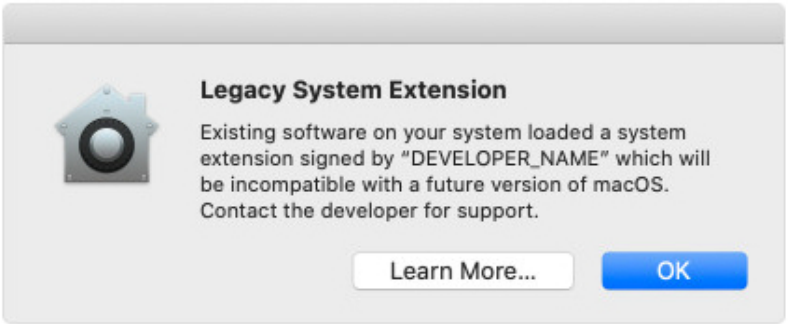
In der Vergangenheit gab es eine Inkompatibilität mit Dropbox, die zu "falschen" Inhalten für kleinere Dateien führen konnte, da Dropbox die letzte Dateiänderung nicht synchronisierte.

- 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*.

Veraltete Systemerweiterung

Systemerweiterungen werden seit vielen Jahren verwendet um die Funktionalität von macOS zu erweitern. Apple arbeitet derzeit an modernen Alternativen zu Systemerweiterungen um die Sicherheit, Stabilität und Zuverlässigkeit in zukünftigen macOS-Versionen zu verbessern.

Boxcryptor verwendet eine Systemerweiterung um das virtuelle Boxcryptor-Laufwerk bereitzustellen. Daher kann Ihnen seit macOS 10.15.4 (Catalina) eine "Veraltete Systemerweiterung"-Nachricht beim ersten Start und später im laufenden Betrieb von Boxcryptor angezeigt werden.



Wir kennen diese Nachricht und Apples Abkehr von Systemerweiterungen in macOS. Wir werden die zukünftigen Anforderungen von Apple rechtzeitig erfüllen.

Bis dahin können Sie diese Nachricht ignorieren und das Fenster getrost schließen. Boxcryptor wird weiterhin mit macOS ohne Probleme funktionieren. Weitere Informationen finden Sie hier.

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.

Systemerweiterungen aktivieren

> Das Aktivieren von Systemerweiterungen ist eine unabdingbare Voraussetzung für die Verwendung von Boxcryptor auf Apple Chip-Macs und sonst wird Boxcryptor nicht funktionieren.

Apple verriegelt macOS mit Apple Chip-Macs weiter, bei denen Kernelerweiterungen von Drittanbietern nun standardmäßig deaktiviert sind. Boxcryptor verwendet eine Kernelerweiterung, um das virtuelle Boxcryptor-Laufwerk bereitzustellen und sich in das Dateisystem von macOS zu integrieren und eine optimale Benutzererfahrung zu gewährleisten. Im Moment kann diese enge Integration in macOS nur durch eine Kernelerweiterung ermöglicht werden.

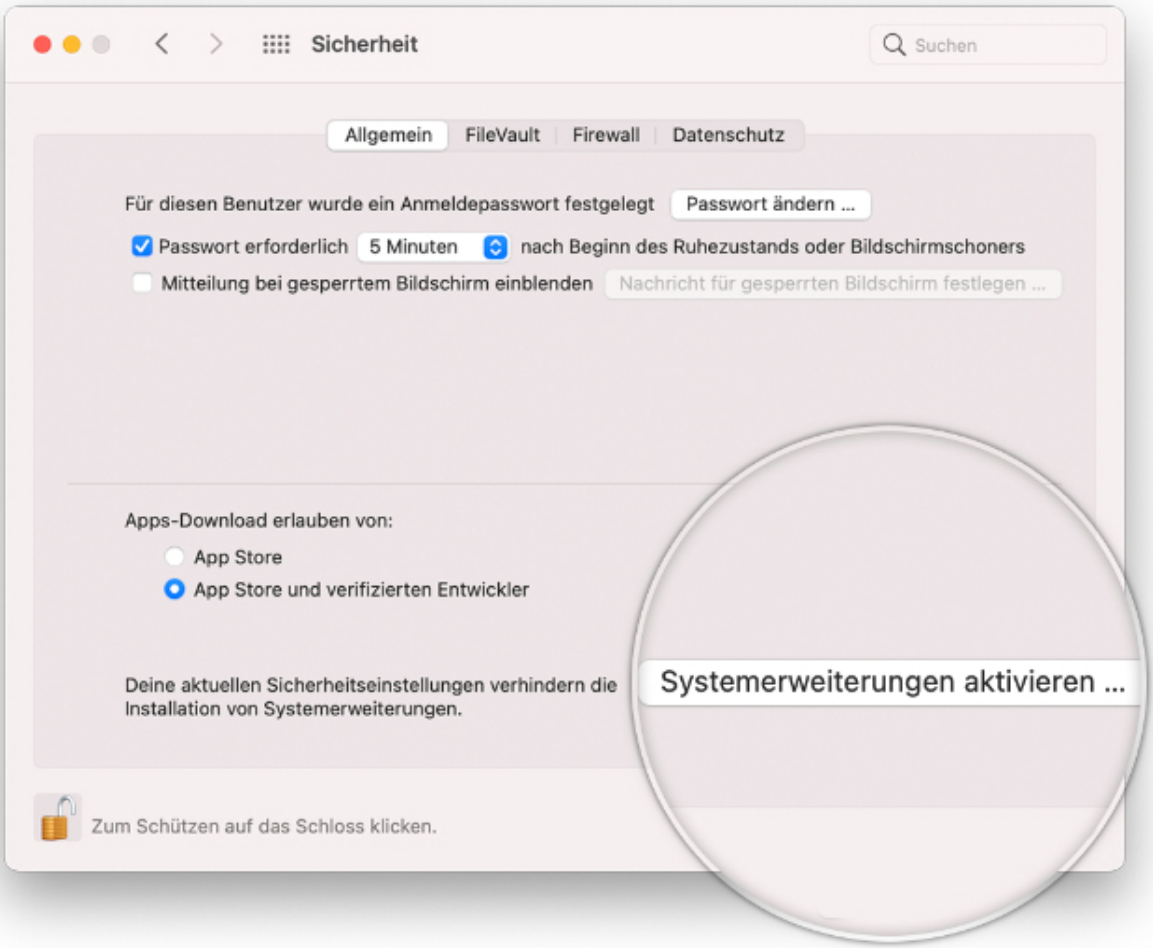
Um Kernelerweiterungen von Drittanbietern auf Apple Chip-Macs zu verwenden, müssen Benutzer Systemerweiterungen aktivieren, indem sie die **Sicherheitsrichtlinie** ihres Macs auf **Reduzierte Sicherheit** ändern und die **Verwaltung von Kernelerweiterungen von identifizierten Entwicklern durch den Benutzer zulassen**. Trotz des dramatischen Namens bietet **Reduzierte Sicherheit** weiterhin die beste Sicherheit für jeden Mac:

Bei **Volle Sicherheit** kann nur die neueste von Apple genehmigte und signierte Version von macOS installiert werden. Bei der (Neu-)Installation von macOS stellt ihr Mac eine Verbindung zu Apples Servern her und prüft, ob die macOS-Version installiert werden darf. Apple kann die Installation einer macOS-Version aus der Ferne verhindern.

Bei **Reduzierte Sicherheit** können nur von Apple genehmigte und signierte Versionen von macOS installiert werden. Im Gegensatz zu **Volle Sicherheit** umfasst dies nicht nur die neueste, sondern auch frühere Versionen von macOS. Es wird keine Verbindung zu Apple Servern hergestellt und Apple kann die Installation einer macOS-Version nicht aus der Ferne verhindern.

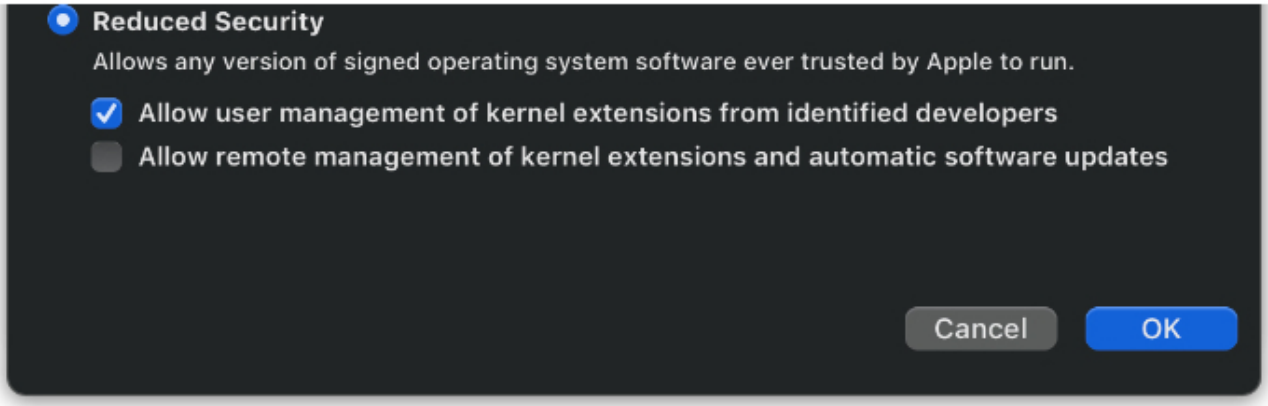
In ähnlicher Weise schwächt die Benutzer-Erlaubnis Kernelerweiterungen von identifizierten Entwicklern zu verwalten nicht an sich nicht die Sicherheit Ihres Macs. **Kernelerweiterungen werden immer noch standardmäßig blockiert und jede Kernelerweiterung muss explizit von einem Benutzer mit Administratorrechten genehmigt werden bevor sie geladen kann.** Darüberhinaus müssen Kernelerweiterungen durch von Apple genehmigten und akkreditierten Entwicklern signiert und notarisiert werden.

Falls erforderlich, werden Sie automatisch aufgefordert, Systemerweiterungen zu aktivieren, wenn Sie Boxcryptor zum ersten Mal auf einem Apple Chip-Mac ausführen. Öffnen Sie in diesem Fall **Sicherheitseinstellungen -> Sicherheit** und folgenden Sie den dortigen Anweisungen.



Alternativ können Sie Systemerweiterungen aktivieren, indem Sie die folgenden Schritte wie von Apple dokumentiert ausführen:

1. Starten Sie Ihren Mac in der macOS-Wiederherstellung
2. Öffnen Sie **Dienstprogramme -> Startsicherheitsdienstprogramm**
3. Wählen und entsperren Sie ihr Systemvolume und klicken Sie auf **Sicherheitsrichtlinien...**
4. Wählen Sie **Reduzierte Sicherheit**
5. Aktivieren Sie **Verwaltung von Kernel-Erweiterungen verifizierter Entwickler durch Benutzer erlauben**
6. Klicken Sie auf **OK** und bestätigen Sie die Aktion durch Eingabe Ihrer Administrator-Anmeldedaten
7. Starten Sie Ihren Mac neu

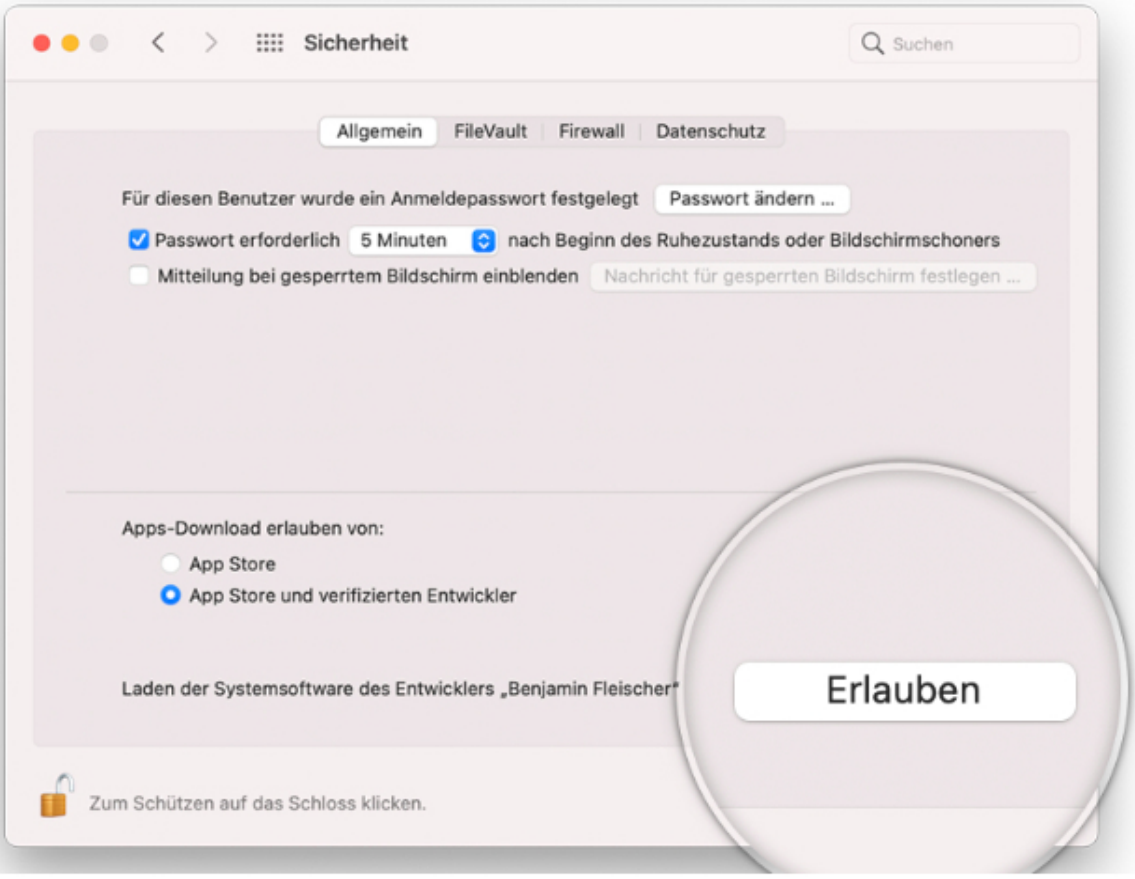


Boxcryptor-Systemerweiterung erlauben

Das Erlauben der Boxcryptor-Systemerweiterung ist eine unabdingbare Voraussetzung für die Verwendung von Boxcryptor und sonst wird Boxcryptor nicht funktionieren.

Die Boxcryptor-Kernel-Erweiterung ist standardmäßig blockiert und muss von einem Benutzer mit Administratorrechten erlaubt werden, bevor sie geladen werden kann. Falls erforderlich, werden Sie beim ersten Start automatisch aufgefordert, die Boxcryptor-Systemerweiterung zu erlauben. Öffnen Sie in diesem Fall **Systemeinstellungen -> Sicherheit** und folgen Sie den dortigen Anweisungen.

Hinweis: Benjamin Fleischer ist der Maintainer der von Boxcryptor verwendeten Open-Source-Kernel-Erweiterung.



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.

> Stellen Sie 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:

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

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 2.46.1667 & 2.46.1668 (2022-03-21)

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

Download v2.46.1668 for macOS 11 - 12

Download v2.46.1667 for macOS 10.15

Version 2.45.1654 & 2.45.1655 (2022-03-14)

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

Download v2.45.1655 for macOS 11 - 12

Download v2.45.1654 for macOS 10.15

Version 2.44.1601 & 2.44.1602 (2022-01-31)

- Added: Support for OneDrive for Mac v22 with updated Files On-Demand experience
- Added: Support for Box Drive on macOS File Provider Extension mode
- Fixed: Opening PDF files in Adobe Acrobat DC may fail on macOS 12.1
- Changed: Removed path length restriction for Microsoft Excel
- Minor bug fixes and improvements

Download v2.44.1602 for macOS 11 - 12

Download v2.44.1601 for macOS 10.15

Version 2.43.1464 & 2.43.1465 (2021-10-14)

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

Download v2.43.1465 for macOS 11 - 12

Download v2.43.1464 for macOS 10.15

Version 2.42.1436 & 2.42.1437 (2021-09-20)

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

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

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

Download v2.42.1437 for macOS 11 - 12

Download v2.42.1436 for macOS 10.15

Version 2.41.1307 & 2.41.1308 (2021-05-31)

- Fixed: Cannot sign in if Google Chrome v91 is the default browser

- Minor bug fixes and improvements

Download v2.41.1308 for macOS 11 Big Sur

Download v2.41.1307 for macOS 10.14 - 10.15

Version 2.40.1233 & 2.40.1234 (2021-03-29)

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

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

Download v2.40.1234 for macOS 11 Big Sur

Download v2.40.1233 for macOS 10.14 - 10.15

Version 2.39.1119 (2020-12-18)

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

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

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

Download

Version 2.38.1090 (2020-12-01)

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

- Reverted: Used space on the Boxcryptor disk includes purgeable space which is actually freed

automatically by macOS if more free space is required

Download

Version 2.38.1086 (2020-11-30)

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

Download

Version 2.37.1043 (2020-11-04)

- Minor bug fixes and improvements

Download

Version 2.36.1042 (2020-10-16)

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

- Added: Support for macOS Big Sur 11.0
- Added: Support for Google Drive shortcuts
- Added: Auto-detection for MagentaCLOUD, CloudMe, SpiderOak, Storegate and Yandex
- Removed: Support for Spotlight (see note below)
- Improved: Compatibility with various backup solutions
- Improved: Symlinks are followed inside the Boxcryptor drive if they target another location
- Changed: Sign out is now part of the account preferences
- - Changed: Updated BCFS to v3.11.2
- Fixed: Administrators could not change permissions to other groups using the Master Key
- Fixed: Local privilege escalation
- Minor bug fixes and improvements

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

Download

Version 2.35.1024 (2020-06-22)

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

Download

Version 2.34.1023 (2020-06-09)

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

Download

Version 2.33.1015 (2020-02-24)

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

Download

Version 2.32.1010 (2019-12-16)

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

Download

Version 2.31.1006 (2019-11-07)

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

Download

Version 2.30.1004 (2019-10-07)

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

Download

Version 2.29.1001 (2019-09-25)

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

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

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

Download

Version 2.28.995 (2019-07-10)

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

Download

Version 2.27.977 (2018-12-18)

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

- Minor bug fixes and improvements

Download

Version 2.26.964 (2018-09-06)

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

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

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

Download

Version 2.25.954 (2018-07-31)

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

Download

Version 2.24.941 (2018-06-14)

- Minor bug fixes and improvements

Download

Version 2.23.939 (2018-05-24)

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

Download

Version 2.22.933 (2018-04-19)

- New: Multi-threaded filesystem
- Added: Russian localization
- Added: Dropbox Team Spaces support
- Added: Compatibility with VirusBarrier v10.9.16 or newer

- Fixed: Standalone OneDrive app is not auto-detected
- Minor bug fixes and improvements

Download

Version 2.21.923 (2018-02-28)

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

Download

Version 2.20.918 (2018-02-13)

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

Download

Version 2.19.907 (2017-12-13)

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

Download

Version 2.18.902 (2017-12-12)

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

Download

Version 2.17.892 (2017-11-23)

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

Download

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

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

Download

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

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

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

Download

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

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

Download

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

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

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

Download

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

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

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

Download

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

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

Download

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

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

Download

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

- Added: Support for Dropbox Smart Sync
- Added: Plaintext overlay icon
- Fixed: Bulk operations (e.g. Manage Permissions) did not handle filename encrypted files or folders with "Umlaute" correctly
- Fixed: Sometimes temporary folders were not deleted when saving a file in MS Office 2016
- Fixed: Saving an encrypted MS Office 2016 file in an unencrypted folder could remove encryption (to avoid any such situation, it is always recommended to store encrypted files within an encrypted folder)
- Fixed: Boxcryptor drive did freeze under certain circumstances
- Changed: Upgraded BCFS to v3.5.6
- Changed: New provisioning profile valid until 2035
- Minor bug fixes and improvements

Download

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

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

Download

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

- Minor bug fixes and improvements

Download

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

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

Download

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

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

Download

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

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

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

Download

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

- Fixed: Spotlight does not include results from Boxcryptor drive in v2.3 versions.
- Improved: Reliability of Finder extension
- Changed: Upgraded BCFS to v3.4.1
- Changed: Due to unexpected issues with Spotlight, the Boxcryptor drive is again mounted under /Volumes instead of the home directory. The new mountpoint is /Volumes/Secomba/{USERNAME}/Boxcryptor where {USERNAME} is the currently logged in macOS username. By default, a symlink is created from ~/Boxcryptor to the new mountpoint and it is recommended to only reference the ~/Boxcryptor symlink in custom scripts to be independent from future mountpoint changes.
- Various other bug fixes and improvements

Download

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

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

Download

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

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

~/Boxcryptor. **(UPDATE 08/05/2016: This change had to be partially reverted in v2.3.405 due to unexpected issues with Spotlight. The new mountpoint is now /Volumes/Secomba/{USERNAME}/Boxcryptor)**

Download

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

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

- Added: Hidden preference "disableAccessControlLists" in order to disable the newly introduced support for Access Control Lists (ACLs) which could give a small performance boost if they are not required.
- Fixed: Sporadic deadlock when accessing ACLs on a symlink whose target is located on the Boxcryptor drive
- Fixed: Sporadic deadlock when setting attributes on a symlink whose target is located on the Boxcryptor drive
- Fixed: If a folder contains an item with a filename represented by more than 255 bytes, also other items are possibly not shown in the Boxcryptor drive. Now only the affected item is not shown but all other items are displayed correctly. In order to show the affected item, shorten its original filename.
- Minor bug fixes and improvements

Download

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

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

Download

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

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

Download

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

- Added: Auto-detection for LiveDrive.
- Added: Support for email addresses with gTLDs.
- Removed: Auto-detection for Wuala.
- Fixed: The file name of an encrypted Office document does not keep its encryption setting if the

document is saved within a plain text folder.
- Fixed: Changing the case of a file or folder name deletes it under certain circumstances.
- Fixed: LiveDrive syncing causes Boxcryptor to create lots of files.
- Fixed: Cannot save a Office document when the path exceeds 255 characters.
- Minor bug fixes and improvements

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

- Minor bug fixes and improvements.

Download

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

- Added: Preliminary support for Mac OS X 10.11 El Capitan (beta)
- Added: Auto-detection for removable devices (e.g. usb flash drives)
- Fixed: Minimized impact of OS X XARA keychain vulnerability by always re-creating keychain items instead of updating existing items.
- Fixed: Finder can't open Excel documents on network locations in some cases.
- Fixed: Deadlock of the Boxcryptor disk when running an executable from the disk.
- Improved: Updated BCFS 3.0.4

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

- Improved: On Yosemite the Boxcryptor context menu is now located directly within the context menu and not in the "Services" menu anymore.
- Improved: On Yosemite the green tag of encrypted files is not copied anymore when copying or moving a file from the Boxcryptor disk to another location.
- Changed: Renamed auto-detected iCloud Drive location to "iCloud Drive (Mac & PC only)" to better guide users where they can access encrypted files in this location. Note: We are working on full iCloud support also on mobile devices which will be available in the next version of Boxcryptor for iOS (ETA in January).
- Fixed: Problems when using Wuala
- Fixed: Boxcryptor disk can deadlock on accessing symlinks in the Boxcryptor disk which have a target in the Boxcryptor disk.
- Minor bug fixes and improvements

Download

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

- Fixed: Issue with desktop alias creation.

Download

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

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

Download

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

- Improved: Better encryption / decryption performance by improved utilization of multi-core systems.
- Improved: The Boxcryptor disk is now always shown in the Finder favorites and on the Desktop.
- Improved: Modifying permission does now retain the original modification date (instead of

setting it to the current date and time).
- Fixed: Enabling Spotlight fails under certain circumstances.
- Fixed: Sign out does not unlink the device
- Minor bug fixes and improvements

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download

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

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

Download: Download

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

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

Download

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

- Minor bug fixes and improvements

Download

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

- Initial Release

Download

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