

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 Voraussetzung und kümmern sich für Sie um die Speicherung Ihrer Dateien. Sie speichern **Ihre Dateien auf deren Servern** und synchronisieren sie auf jedes verbundene Gerät.

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

Was ist Boxcryptor?

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



Was Boxcryptor **nicht** ist

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

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

Quickstart

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

Boxcryptor installieren

Systemvoraussetzungen: Benötigt mindestens Windows 10, [.NET Framework >= 4.7.2](#) und [WebView2 Runtime](#) (Wenn Sie Windows regelmäßig updaten, haben Sie .NET Framework sowie die WebView2 Runtime wahrscheinlich schon installiert).



Derzeit läuft Boxcryptor nicht nativ auf **ARM**-basierten Windows 10 / 11-Geräten. Wir arbeiten jedoch daran, die ARM-Architektur in naher Zukunft zu unterstützen.



Boxcryptor wird offiziell nicht auf **Windows Insider Previews** unterstützt. Diese experimentellen Windows Versionen können ohne vorherige Warnungen Apps unbrauchbar machen. Sollten Sie Probleme haben, finden Sie Abhilfe unter [Zurückkehren zur vorherigen Windows-Version](#).

Um Boxcryptor auf Ihrem Windows-PC zu installieren, folgen Sie diesen drei Schritten:

1. Installieren Sie die Desktopanwendung Ihres Cloud-Anbieters.
2. Laden Sie [Boxcryptor für Windows](#) herunter.
3. Starten Sie den Installer und folgen Sie den Anweisungen.

Anschließend werden Sie gefragt, ob Sie einen Gerätetreiber von der Callback Technologies (vormals EldoS Corporation) installieren wollen. Dieser ist eine **notwendige** Komponente von Boxcryptor. Klicken Sie deshalb bitte auf **Installieren**. Der Installer wird dann vorübergehend einige Anwendungen schließen. Nach der Installation werden diese automatisch wieder geöffnet.

Ein Boxcryptor-Konto erstellen



Mit dem Anschluss [Boxcryptors an Dropbox](#) können keine neuen Boxcryptor-Konten erstellt werden.

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

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

Wählen Sie ein Passwort, das Sie sich merken können oder bewahren Sie das Passwort an einem sicheren Ort auf, wie zum Beispiel einem Passwortmanager. Boxcryptor folgt dem Zero-Knowledge-

Prinzip, daher können wir Ihr Passwort **nicht** zurücksetzen.

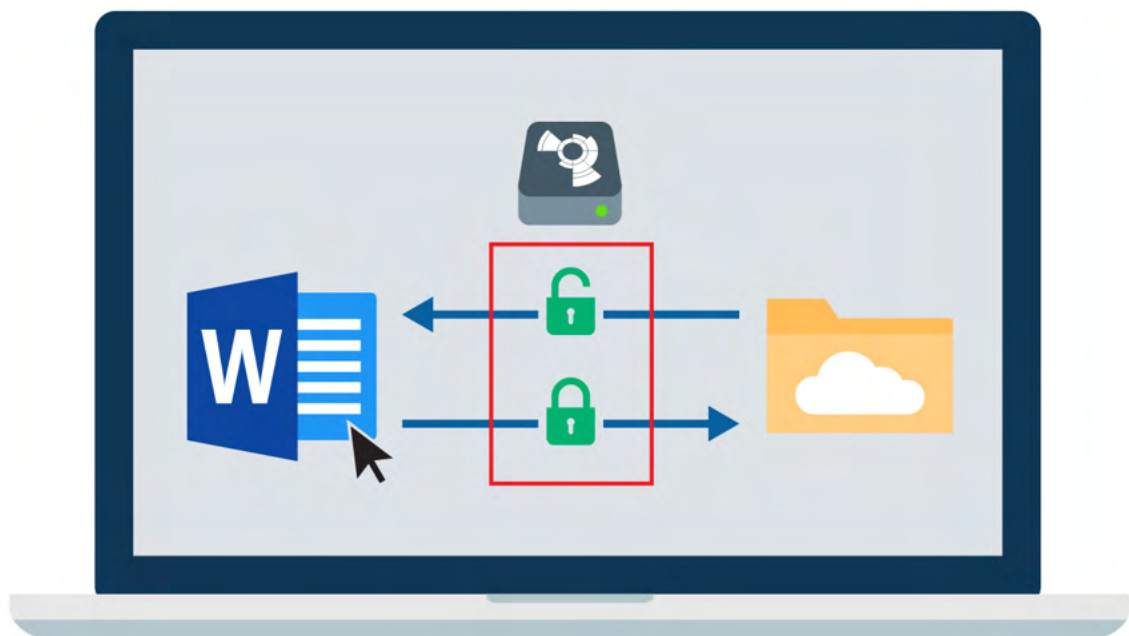



Wenn Sie Ihr Passwort vergessen, sind Ihre Daten irreversibel verloren.

Entdecken Sie Boxcryptor

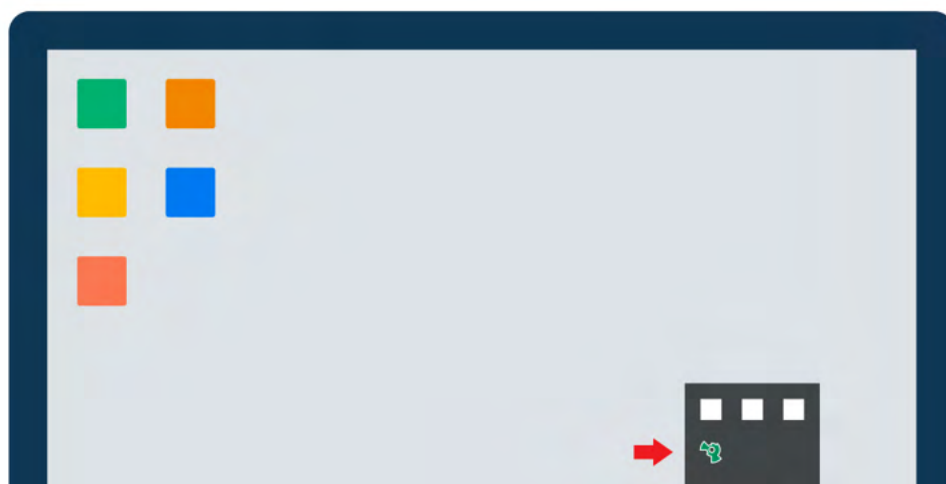
Nachdem Sie Boxcryptor installiert und sich mit Ihrem Boxcryptor Konto angemeldet haben, können Sie auf das **Boxcryptor-Laufwerk** mit dem Laufwerksbuchstaben **X** zugreifen:

Boxcryptor fügt **automatisch** alle installierten Cloud-Anbieter zum Laufwerk hinzu. Ab jetzt finden Sie alle Ihre Cloud-Speicher hier. Das Laufwerk ist eine zusätzliche Ebene über Ihren vorhandenen Dateien. 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 per Doppelklick auf das Boxcryptor-Symbol in der Systemleiste direkt neben der Uhrzeit.





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.

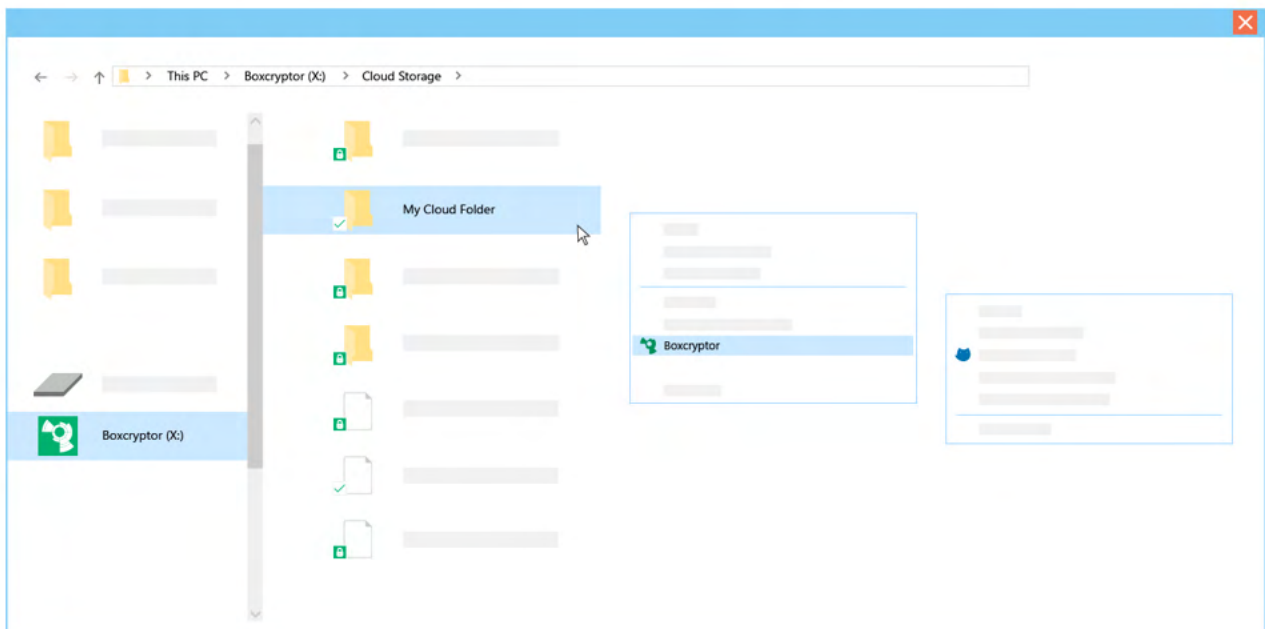
1. Öffnen Sie Ihr **Boxcryptor-Laufwerk**.
2. Öffnen Sie darin den Ordner Ihres Cloud-Anbieters.
3. Klick auf **+ Neu → Ordner**.
4. Wenn Sie einen verschlüsselten Ordner erstellen möchten, bestätigen Sie mit einem Klick auf **Ja**.
5. Fügen Sie dem Ordner Dateien hinzu. Alle Dateien werden automatisch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



Wie man bestehende Dateien verschlüsselt

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

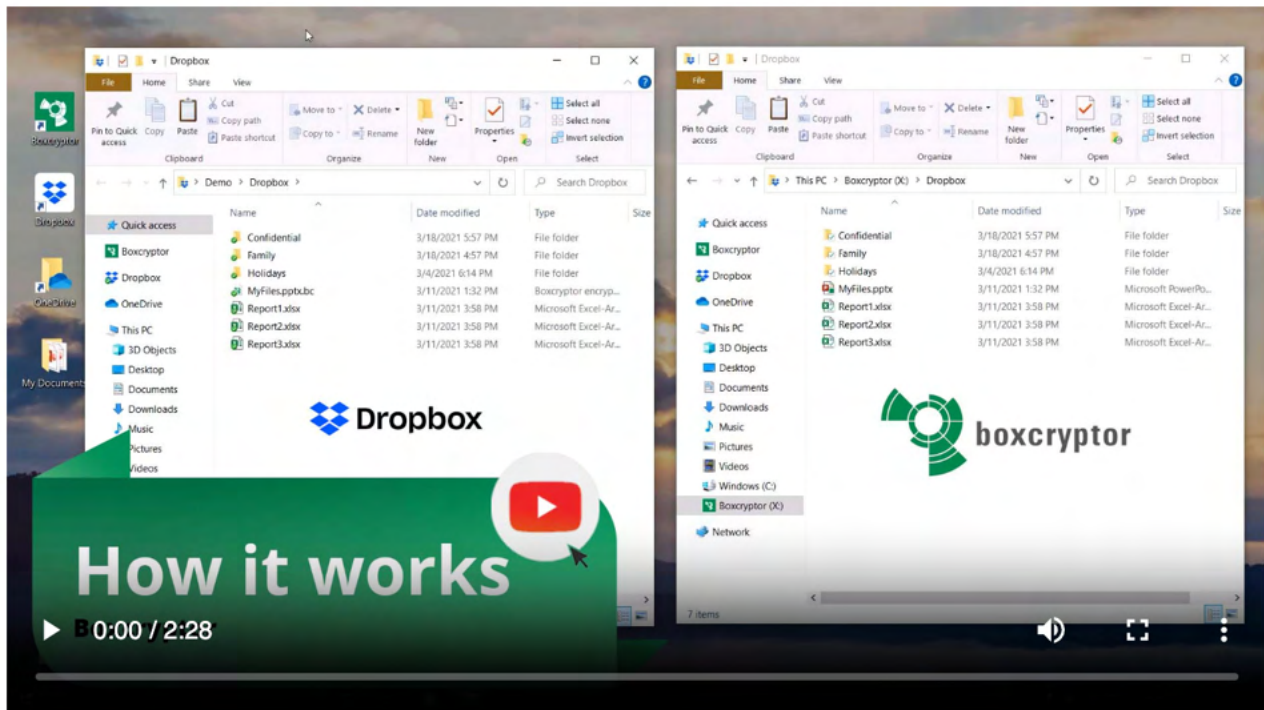
1. Navigieren Sie in Ihr **Boxcryptor-Laufwerk**.
2. **Rechtsklick** auf eine Datei oder einen Ordner → **Boxcryptor** → **Verschlüsseln**.
3. Warten Sie, bis der Sync-Client Ihres Cloud-Anbieters **alles synchronisiert hat**.



Hinweis: Die Overlay-Symbole im Boxcryptor-Laufwerk werden Ihnen anzeigen, wann die Synchronisierung und Verschlüsselung abgeschlossen sind. Dies funktioniert jedoch nur, wenn Ihr Cloud-Anbieter diese Funktion unterstützt.



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.



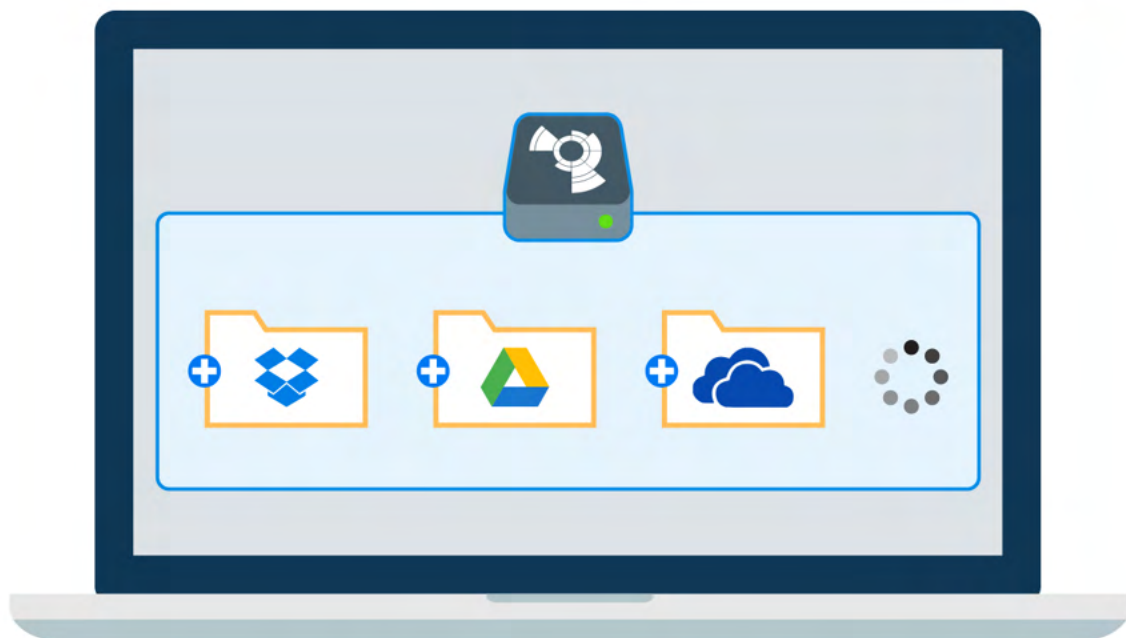
Verwalten Sie Ihre Clouds und Speicherorte

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 synchronisiert. 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 das **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](#).

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**



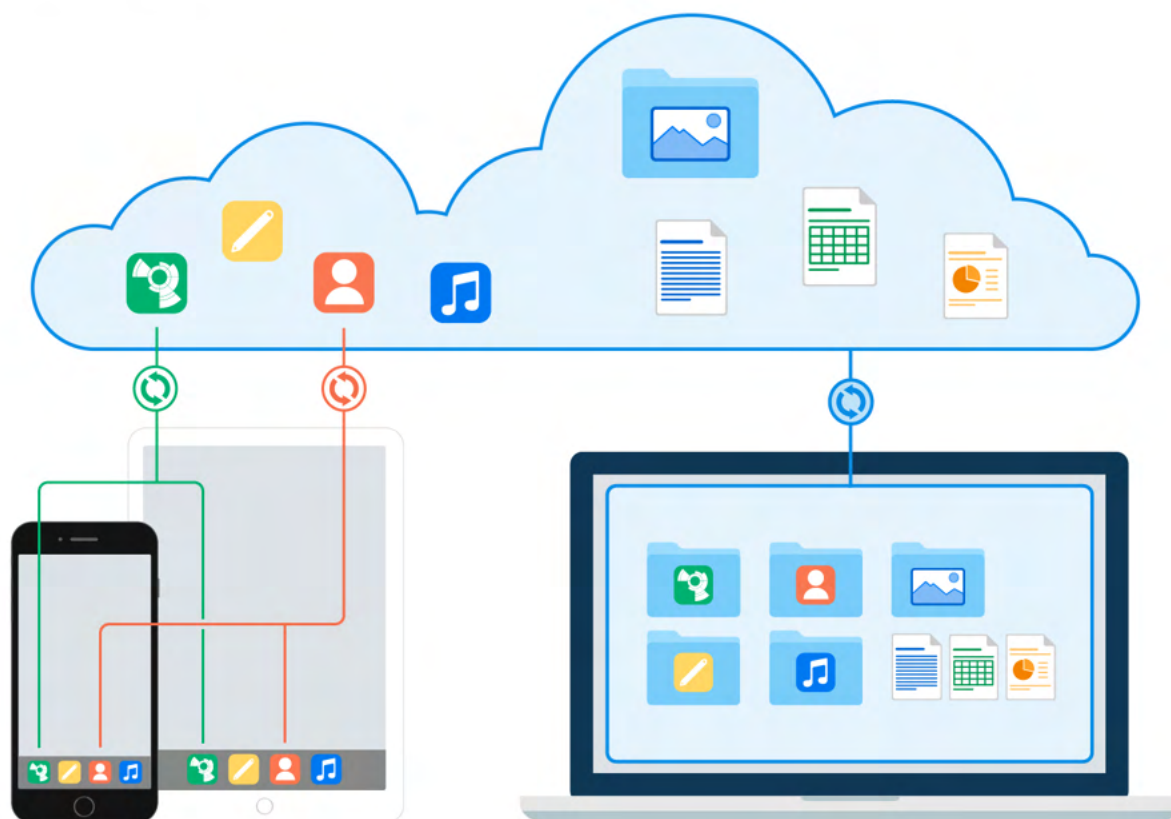
synchronisiert wurden. Ordner aus **Mein Computer** sind auf anderen Computern sowie in den mobilen Boxcryptor-Apps nicht zugänglich. Wenn Sie Dateien in einem gesicherten Ordner verschlüsseln möchten, können Sie ihn manuell als [benutzerdefinierter Speicherort](#) hinzufügen.



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

iCloud

Die Tatsache, dass es einen iCloud Drive (ein typischer Cloud-Anbieter) und zusätzlich eine iCloud gibt (wo alle Ihre Apps und deren von Apple verwaltete Cloud-Speicher liegen), macht die plattformübergreifende Einrichtung der Verschlüsselung etwas komplexer als bei anderen Cloudlösungen. Einige zusätzliche Schritte sind bei der Einrichtung notwendig. Nachdem jedoch Boxcryptor für die iCloud einmal eingerichtet wurde, ist der Umgang damit genauso einfach wie bei anderen Anbietern.



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

Wie Sie iCloud Drive verschlüsseln und Ihre Daten auf Mobil- und Desktopgeräten verfügbar machen

Wenn Sie Zugriff auf Ihre verschlüsselten Daten auf all Ihren Geräten haben wollen, führen Sie die nachfolgenden Schritte aus:

1. Installieren Sie Boxcryptor auf Ihrem iPhone oder iPad und zusätzlich auf Ihrem Desktop-Gerät.
2. Stellen Sie sicher, dass Sie auf allen Geräten mit dem gleichen Konto bei iCloud angemeldet sind.
3. Fügen Sie **iCloud** in Boxcryptor für iOS hinzu.
4. Laden Sie eine verschlüsselte Datei in **iCloud** über Boxcryptor für iOS hoch.
5. Apple erstellt einen Ordner für Boxcryptor in Ihrer iCloud.
6. Öffnen Sie Boxcryptor auf Ihrem Desktop-Gerät und öffnen Sie Ihren **iCloud**-Speicherort auf macOS oder **iCloud Drive** → **Boxcryptor** auf Windows. Sie finden dort Ihre verschlüsselte Datei von Ihrem iPhone oder iPad.
7. Um Ihre Dateien von Ihrem Mac oder PC auf Ihrem iPhone oder iPad verfügbar zu machen, kopieren Sie diese in die oben erwähnten Ordner. Danach sind Sie auch auf Ihrem iPhone oder iPad verfügbar.

Netzlaufwerke und USB-Geräte

Netzlaufwerke und USB-Wechseldatenträger werden von Boxcryptor ebenfalls automatisch erkannt. Da Netzlaufwerke nicht immer verfügbar sind wenn Boxcryptor läuft, werden sie nicht automatisch entfernt. Die Auto-Detect-Funktion muss vorübergehend abgeschaltet werden, um alte Netzlaufwerke zu entfernen.

✓ Wie Sie die Auto-Detect-Funktion für Laufwerke abschalten

- Rechtsklick auf Boxcryptor Tray Symbol → Einstellungen → Erweitert → **Weitere Einstellungen**.
- Auto-Detect Wechsellaufwerke oder Auto-Detect Netzlaufwerke ausschalten.

Benutzerdefinierte Speicherorte

Falls Ihre bevorzugte Cloud nicht als [unterstützter Anbieter](#) aufgeführt ist oder falls Sie einen bestimmten Ordner auf Ihrem Rechner verschlüsseln möchten, können Sie das ebenfalls tun:

Klicken Sie mit der rechten Maustaste auf **das Boxcryptor Taskleistensymbol** → **Einstellungen** → **Speicherorte** → **Hinzufügen** und wählen Sie dann Ihren Speicherort aus.



Falls der von Ihnen gewählte Speicherort kein Ordner ist, der von einem Cloud-Anbieter synchronisiert wird, wird auch nichts in die Cloud hochgeladen. Die Daten verbleiben lokal aber verschlüsselt auf Ihrem PC.

WebDAV-Speicherorte

Sie können jeden Cloud-Anbieter zu Boxcryptor hinzufügen, wenn dieser WebDAV, oder SMB-Ziele unterstützt:

- Rechtsklick auf das **Boxcryptor Symbol in der Systemleiste** → **Einstellungen** → **Speicherorte** → **Hinzufügen**.
- Geben Sie die korrekte **URL** in der **Adressleiste** des Ordners ein.



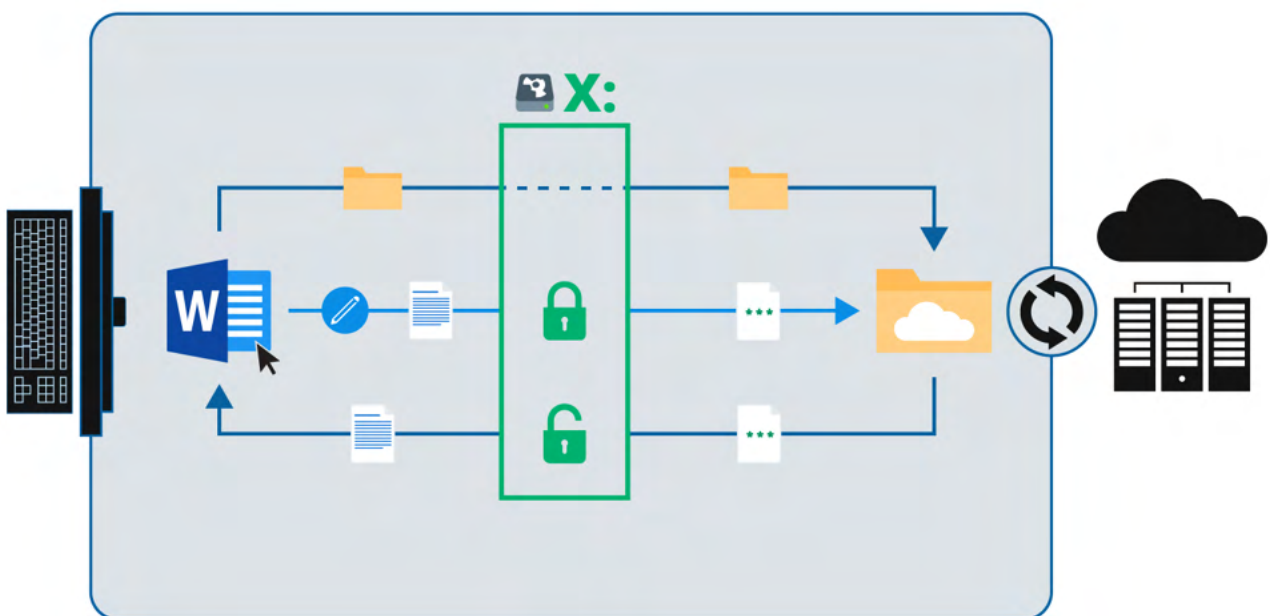
Abhängig von der Latenz und der Bandbreite Ihres Netzwerkes oder Ihrer Internetverbindung kann das Hinzufügen eines Netzwerk-Speicherortes einen erheblichen, negativen Einfluss auf die gesamte Boxcryptor-Performance haben. Daher ist ein lokaler Ordner einem Netzwerk-Speicherort zu bevorzugen.

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 **einzel**n 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.



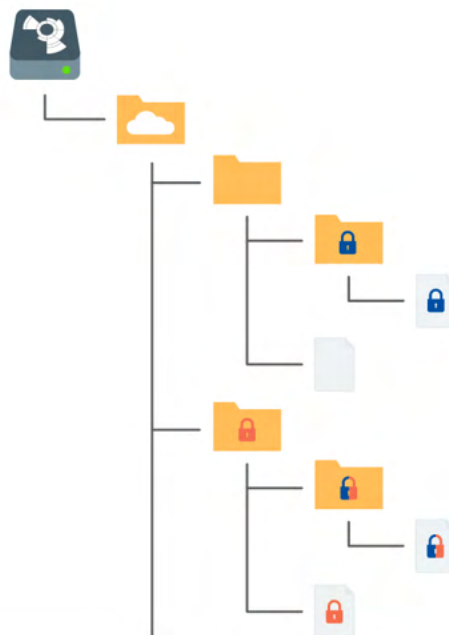
Wir erreichen diese Einfachheit durch die Erstellung eines virtuellen Laufwerks auf Ihrem Computer. Es funktioniert wie ein **zur Verschlüsselung fähiges Fenster zu Ihren Daten**. Auf all Ihre Dateien – unabhängig davon, ob sie verschlüsselt sind oder nicht – kann **über dieses virtuelle Boxcryptor-Laufwerk 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. Zur tiefen Integration in Windows erstellt Boxcryptor ein virtuelles Laufwerk. Die Verschlüsselung erfolgt **on-the-fly**. Dadurch arbeiten alle Programme, inklusive Windows Explorer, **genauso wie mit Daten auf Ihrer Festplatte**.

Um mit verschlüsselten Dateien zu arbeiten, öffnen Sie lediglich das Boxcryptor Laufwerk im **Windows Explorer** und ändern, lesen, kopieren oder verschieben Sie Dateien wie in einem ganz normalen Ordner.



Falls Sie keine Boxcryptor-Berechtigung haben um eine Datei zu öffnen, werden Ihnen einige Programme Fehlermeldungen wie «ungültiger Parameter» oder «kann nicht geöffnet werden» anzeigen. In diesem Fall prüfen Sie bitte die Berechtigung indem Sie die **mit der rechten Maustaste auf die Datei oder den Ordner klicken und → Boxcryptor → Berechtigungen verwalten auswählen**. Weitere Informationen finden Sie unter [Teilen mit Boxcryptor-Nutzern](#).

Wie Sie verschlüsselte Dateien erkennen

Boxcryptor ermöglicht es Ihnen, **verschlüsselte und unverschlüsselte** Dateien und Ordner im gleichen Verzeichnis zu verwalten. Verschlüsselte Dateien und Ordner im Boxcryptor-Laufwerk sind

mit kleinen Icons markiert, die den aktuellen Zustand zeigen.

 **verschlüsselt** und **synchronisiert**

 **verschlüsselt** und **Synchronisation im Gange**



Dropbox Smart Sync Online-only-Dateien werden im Boxcryptor-Laufwerk leicht ausgegraut angezeigt. Siehe [On-Demand-Dateien](#) für weitere Informationen.

Verschlüsselung vorhandener Dateien und Ordner

Wenn Sie bereits Dateien in Ihrer Cloud haben, können Sie diese nachträglich verschlüsseln. Und so funktioniert es:

- Navigieren Sie zu der Datei oder dem Ordner, den Sie verschlüsseln möchten.
- Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner und wählen Sie **Boxcryptor** → **Verschlüsseln** im Kontextmenü.
- Warten Sie, bis die Anwendung Ihres Cloud-Anbieters alles synchronisiert hat.



Bitte **warten Sie bis die Anwendung Ihres Anbieters die Datei synchronisiert hat**, bevor Sie mit dieser arbeiten. Damit verhindern Sie Synchronisationskonflikte.

Hinweis: Um Synchronisationskonflikte zu vermeiden, hängt Boxcryptor das Suffix **_encrypted** an den Namen der Datei oder des Ordners an. Nachdem die Synchronisation beendet ist, können Sie den Namen ohne Probleme wieder ändern.

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: 恠悰捥抱峇珍殍相瞻
擲馭漢快搬濂濂湮惶掙挹柜櫟秘.bc

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

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

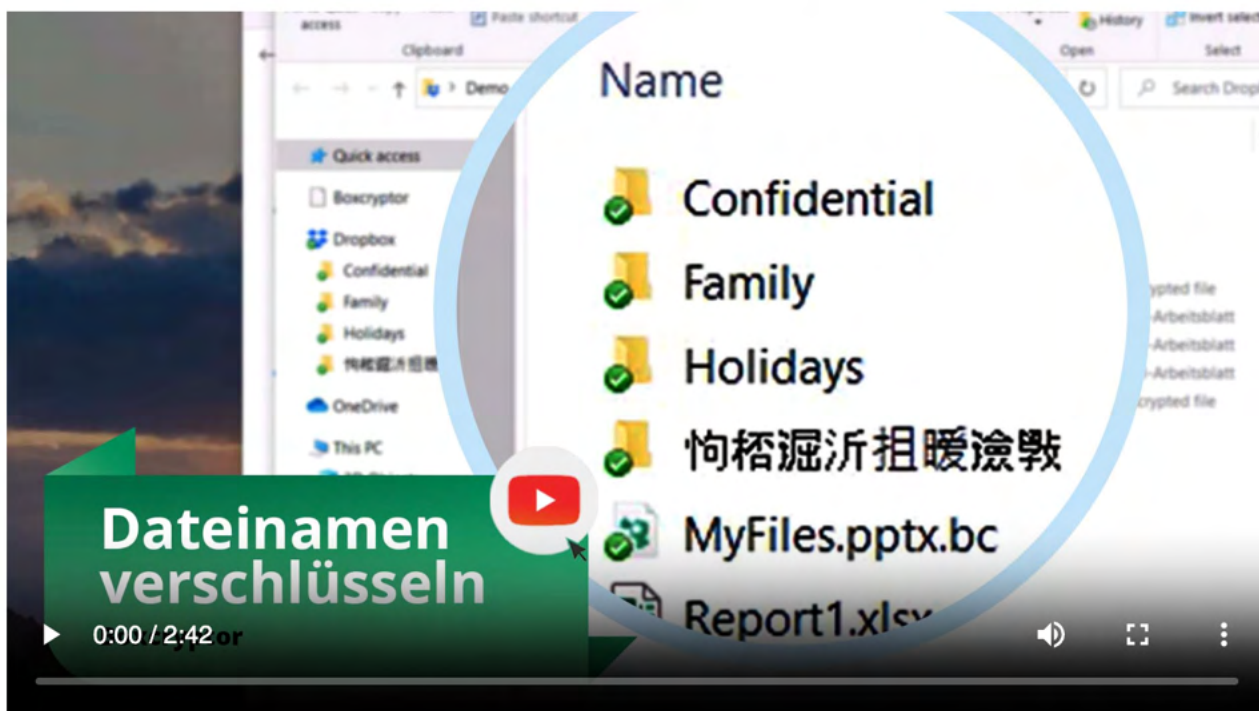
Dateinamenverschlüsselung gespeichert wird, ebenfalls Dateinamenverschlüsselung haben.



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

Um die Dateinamenverschlüsselung global zu aktivieren, gehen Sie auf **Boxcryptor Einstellungen** → **Sicherheit** → **Verschlüsselung** und wählen Sie **Dateinamenverschlüsselung aktivieren**.

Um die Dateinamenverschlüsselung bei bereits bestehenden Dateien zu aktivieren, rechtsklicken Sie diese, wählen Sie **Boxcryptor** → **Dateinamenverschlüsselung aktivieren / deaktivieren** im Kontextmenü. Folgen Sie den Anweisungen und stellen Sie sicher, dass der Sync komplett abgeschlossen ist, bevor Sie weiter mit diesen Dateien arbeiten.



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, dass nicht alle Dateien automatisch mit Ihrem Gerät synchronisiert werden. Stattdessen wird nur die Verzeichnisstruktur auf Ihrem Gerät repliziert und die Dateien werden on-Demand heruntergeladen, sobald Sie sie öffnen. Somit werden wertvoller Speicherplatz und Bandbreite gespart, während Sie trotzdem von Ihrem Computer aus Zugang zu jeder Datei haben.

Dropbox Smart Sync

Dropbox Smart Sync definiert drei Zustände für Dateien und Ordner:

- **Nur online verfügbare Inhalte** werden in Ihrem lokalen Dropbox-Ordner angezeigt, verwenden aber nicht den vollen Speicherplatz, der für die Datei benötigt würde. In Ihrem Explorer können Sie die Dateien sehen, der Inhalt wird aber erst komplett heruntergeladen, wenn Sie ihn brauchen. Nur Dateiinformationen wie Dateiname, Speicherplatz und Update-Datum werden heruntergeladen.
- **Gemischte Ordner** enthalten sowohl lokal gespeicherte Inhalte als auch nur online verfügbare Inhalte.
- **Lokale Inhalte** werden auf die Festplatte Ihres Computers heruntergeladen und gespeichert. Sie können diese Dateien direkt in den Applikationen auf Ihrem Computer editieren.

Boxcryptor bewahrt den Smart-Sync-Zustand der Dateien in Dropbox, lädt Dateien via Dropbox herunter, wenn eine andere Applikation eine nur online verfügbare Datei öffnet und zeigt den Smart-Sync-Zustand im Boxcryptor-Laufwerk an.

Der Smart-Sync-Zustand der Dateien wird anhand des Dateisymbols angezeigt. Das Symbol für Dateien, die nur online verfügbar sind, ist blass oder blass hinterlegt.

Hinweis: Der Dropbox-Smart-Sync Zustand von Ordnern wird im Boxcryptor Laufwerk nicht angezeigt. Wenn Sie den Zustand bestimmen wollen, wählen Sie einen Ordner mit Rechtsklick aus und wählen Sie **Boxcryptor** → **Zeige Original in Dropbox**. Sie können den Smart-Sync-Zustand mit Hilfe der Dropbox-Symbolüberlagerung wie [hier](#) beschrieben erkennen.

Nur online verfügbare Dateien öffnen

Sie können im Boxcryptor-Laufwerk eine Datei, die nur online verfügbar ist, anwählen und direkt öffnen. Boxcryptor wird automatisch einen Download mit Dropbox Smart Sync auslösen und warten, bis die Datei heruntergeladen ist. Wenn der Download beendet ist, wird der Öffnungsprozess weitergeführt. Wenn der Download länger als 3 Sekunden dauert, wird Boxcryptor den Öffnungsprozess abbrechen um die Funktionalität des Boxcryptor-Laufwerks zu bewahren. Sie können den Fortschritt des Öffnungsprozesses im **Dropbox-Menü** verfolgen und sobald der Download beendet ist, können Sie erneut versuchen, die Datei zu öffnen.

Nur online verfügbare Dateien herunterladen

Wenn Sie eine Datei, die nur online verfügbar ist, auch lokal verfügbar machen möchten, ohne die Datei zu öffnen, können Sie mit Rechtsklick auf jede beliebige Datei **Boxcryptor** → **Herunterladen** auswählen. Bitte beachten Sie, dass es zur Zeit aufgrund von Restriktionen bei Dropbox nicht möglich ist, diese Aktion in umgekehrter Reihenfolge durchzuführen, also eine lokale Datei nur online verfügbar zu machen. Um diese Aktion durchzuführen, nutzen Sie bitte Dropbox direkt. Zur

Originaldatei gelangen Sie ganz einfach durch Rechtsklick auf die Datei im Boxcryptor-Ordner. Wählen Sie **Boxcryptor** → **Zeige Original in Dropbox**.

✓ Kann ich die Zugriffsrechte von nur online verfügbaren Ordnern verwalten?

Zugriffsrechte finden sich in der Datei FolderKey.bch innerhalb eines Ordners. Wenn diese Datei nur online verfügbar ist, wird sie automatisch von Dropbox heruntergeladen, sobald der Dialog für die Verwaltung von Zugriffsrechten geöffnet wird. Falls die Datei aufgrund einer fehlenden Internetverbindung nicht heruntergeladen werden kann, können die Zugriffsrechte nicht geändert werden. In diesem Fall stellen Sie bitte eine Onlineverbindung her und versuchen Sie es erneut.

✓ Warum lässt sich eine Office Anwendung (Word, Excel, Powerpoint) nur sehr langsam öffnen?

Wenn Sie eine Office Anwendung öffnen, versucht diese alle kürzlich geöffneten Dateien zu lesen. Wenn diese Dateien nur online verfügbar sind, lädt Dropbox diese herunter und blockiert den Öffnungsprozess bis der Download beendet ist. Um dieses Problem zu umgehen empfiehlt es sich, die Liste der kürzlich geöffneten Dateien in der Office-Anwendung zu löschen.

✓ Warum sind manche Dateien immer lokale Dateien, selbst nachdem ich sie nur online verfügbar gemacht habe?

Bitte lesen Sie hierzu die vorhergehende Frage. Wenn eine Datei in der Liste der kürzlich geöffneten Dateien in der Office-Anwendung aufgeführt ist, wird Dropbox sie beim Öffnen der Anwendung immer herunterladen. Um dieses Problem zu umgehen empfiehlt es sich, die Liste der kürzlich geöffneten Dateien in der Office-Anwendung zu löschen.

✓ Wann brauche ich eine Internetverbindung um mit Smart Sync zu arbeiten?

Sie benötigen eine Internetverbindung wenn Sie eine Datei, die nur online verfügbar ist, öffnen möchten, oder wenn Sie in einem verschlüsselten Ordner arbeiten, dessen Verschlüsselungsdatei (FolderKey.bch) nur online verfügbar ist. Wir empfehlen Ihnen einen verschlüsselten Ordner entweder nur lokal zu speichern oder nur online verfügbar zu machen um gemischte Ordner zu umgehen wenn Sie eine schlechte Internetverbindung erwarten.

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

Nein, wenn Sie im Boxcryptor-Laufwerk arbeiten, ist es gegenwärtig nicht möglich, eine Datei oder einen Ordner nur online verfügbar zu machen. Wenn Sie eine Datei oder einen Ordner nur online verfügbar machen wollen, müssen Sie direkt zum Dropbox-Ordner gehen und im Dropbox Kontextmenü **Smart Sync** → **Nur online verfügbar** wählen. Um eine Datei oder einen Ordner im Dropbox-Ordner zu identifizieren, machen Sie einen Rechtsklick und wählen Sie **Boxcryptor** → **Zeige Original in Dropbox**.

- ✓ Kann ich einen Ordner im Boxcryptor-Laufwerk herunterladen?

Ja! Klicken Sie dazu im Kontextmenü des Ordners auf **Boxcryptor** → **Download**. Dadurch werden alle Dateien rekursiv heruntergeladen. Beachten Sie, dass dadurch nur der aktuelle Stand heruntergeladen wird, zukünftige, der Dropbox aus der Ferne hinzugefügte Dateien, werden nicht automatisch heruntergeladen.

- ✓ Kann ich mit der Windows Suche nur online verfügbare Dateien suchen?

Sie können nur online verfügbare Dateien nach Namen suchen, aber Sie können nicht nach Inhalten suchen, da nur online verfügbare Dateien streng genommen keinen Inhalt haben.

OneDrive Files On-Demand

[OneDrive Files On-Demand](#) wird seit dem Fall Creators Update von Windows 10 offiziell unterstützt.

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

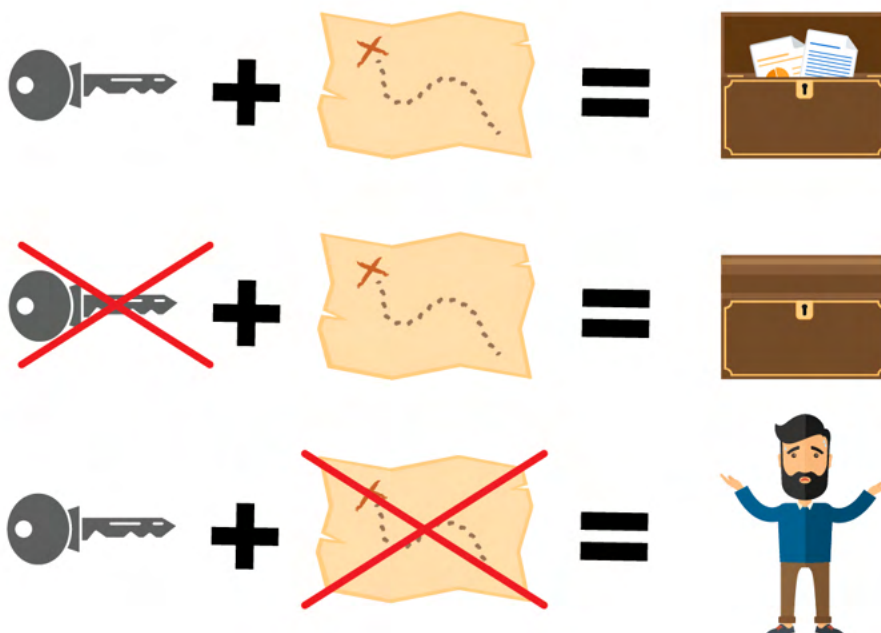
Um zu verstehen, wie das Teilen von verschlüsselten Dateien funktioniert, ist es hilfreich zu wissen, wie Programme unverschlüsselte und verschlüsselte Dateien behandeln.

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 modifiziert. 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**.

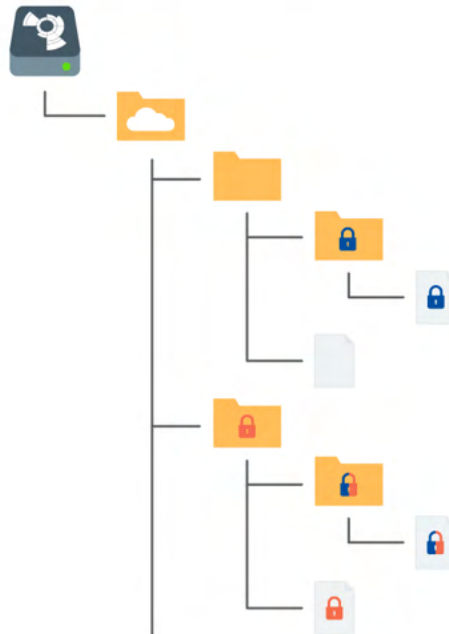
Deshalb sind zwei Schritte nötig, um eine verschlüsselte Datei zu teilen:

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

Mit Boxcryptor können Sie verschlüsselte Dateien mit anderen Boxcryptor-Nutzern teilen.



Wir empfehlen Ihnen, verschlüsselte Ordner nicht direkt mit anderen Personen zu teilen. Insbesondere wenn Sie die Dateinamenverschlüsselung aktiviert haben, ist es besser, wenn Sie den verschlüsselten Ordner in einen unverschlüsselten Ordner verschieben und diesen freigeben.

Neue Dateien oder Ordner (empfohlen)

1. Erstellen Sie einen unverschlüsselten Stammordner.
2. Erstellen Sie einen verschlüsselten Ordner in diesem Stammordner.
3. Klicken Sie mit einem Rechtsklick auf die Datei oder den Ordner und wählen Sie im Kontextmenü **Boxcryptor** → **Berechtigungen verwalten**.
4. Fügen Sie die Nutzer oder Gruppen hinzu, mit denen Sie die Datei oder den Ordner teilen wollen und bestätigen Sie Ihre Auswahl mit **Anwenden**.
5. Kopieren Sie die neuen Dateien oder Ordner in den verschlüsselten Ordner.
6. Geben Sie den **unverschlüsselten Stammordner** bei Ihrem Cloud-Anbieter frei.

Vorhandene unverschlüsselte Dateien oder Ordner

1. Erstellen Sie einen neuen unverschlüsselten Stammordner.
2. Erstellen Sie einen neuen verschlüsselten Ordner in diesem Stammordner.
3. Klicken Sie mit einem Rechtsklick auf den **verschlüsselten Ordner** → **Boxcryptor** → **Berechtigungen verwalten**.
4. Fügen Sie die Nutzer oder Gruppen hinzu mit denen Sie die Datei oder Ordner teilen wollen und bestätigen Sie die Änderungen.
5. Kopieren Sie die vorhandenen, unverschlüsselten Dateien in den verschlüsselten Ordner.
6. Löschen Sie die vorhandenen unverschlüsselten Dateien.
7. Teilen Sie den **unverschlüsselten Stammordner** bei ihrem Cloud-Anbieter.

Vorhandene verschlüsselte Ordner

1. Erstellen Sie einen neuen unverschlüsselten Stammordner.
2. Verschieben Sie den verschlüsselten Ordner in diesen Stammordner.
3. Warten Sie bis die Änderungen von ihrem Cloud-Anbieter synchronisiert wurden.
4. Klicken Sie mit einem Rechtsklick auf den **verschlüsselten Ordner** → **Boxcryptor** → **Berechtigungen verwalten**.
5. Fügen Sie die Nutzer oder Gruppen hinzu mit denen Sie die Datei oder Ordner teilen wollen und bestätigen Sie die Änderungen.
6. Warten Sie bis die Änderungen von ihrem Cloud-Anbieter synchronisiert wurden.
7. Teilen Sie den **unverschlüsselten Stammordner** bei ihrem Cloud-Anbieter.



Wir empfehlen bei der Berechtigungsverwaltung Gruppen zu nutzen, da diese den Synchronisationsaufwand ihres Cloud-Anbieters reduzieren können wenn Sie für einzelne Nutzer Zugriffe erlauben oder entziehen. Mehr Informationen erhalten Sie unter [Vorteile von Gruppen](#).

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. Finden Sie heraus, wie Sie Whisply mit Boxcryptor verwenden [hier](#).

Gruppen verwalten

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



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

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

Vorteile von Gruppen

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

Vorteile von Gruppen:

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

Einstellungen

App-Schutz

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 Boxcryptor auf die Werkseinstellungen zurücksetzen um fortzufahren.

Aus diesen Authentifizierungsmethoden können Sie wählen:

- **vierstelliger PIN-Code:** Wenn festgelegt, müssen Sie einen vierstelligen PIN Code eingeben.
- **Password:** Wenn festgelegt, müssen Sie Ihr Boxcryptor-Password eingeben.



Ist die Anmeldung in Boxcryptor über Single Sign-On erfolgt, ist kein Boxcryptor Password gesetzt und somit die Password-Authentifizierungsoption nicht verfügbar.

Boxcryptor erfordert, dass Sie die Authentifizierung beim Start eingeben. Danach läuft Boxcryptor, bis Sie die Software gezielt verlassen. Falls Sie Boxcryptor schützen möchten, wenn Sie sich von Ihrem Gerät entfernen, verwenden Sie bitte die Funktionen Ihres Betriebssystems, um Ihr Gerät manuell oder automatisch nach einer bestimmten Zeitspanne zu sperren.

Sie können die App-Sperre in den Einstellungen aktivieren und einrichten: **Boxcryptor tray icon → Einstellungen → Sicherheit.**

Bemerkung: Wenn ein Angreifer Zugang zu Ihrem Betriebssystem erhält, ist es theoretisch möglich, die lokal gespeicherten Boxcryptor-Einstellungen so zu verändern, dass die App-Sperre umgangen werden kann. Während diese Funktion Ihnen helfen kann, Ihre verschlüsselten Daten auf Ihrem Computer besser zu schützen, garantiert es jedoch nicht 100%ige Sicherheit gegen anspruchsvolle Angreifer mit Zugriff auf Ihr Betriebssystem. Wir empfehlen, die Best Practices Ihrer Geräte zu beachten, um eine solche Situation zu vermeiden.

Boxcryptor-Einstellungen

Mit einem Rechtsklick auf das Boxcryptor-Symbol in der Systemleiste und der Auswahl von Einstellungen gelangen Sie in die Boxcryptor Einstellungen. Wählen Sie den Tab **Erweitert** aus, um die Bezeichnung des Boxcryptor-Laufwerks, den Laufwerksbuchstaben, Autostart und Update-Einstellungen sowie Dateinamenverschlüsselungsoptionen zu ändern.

Die Standardeinstellungen sind:

- Mit Windows starten

- Nach Updates suchen
- Dateien und Ordner mit einem Punkt am Anfang verstecken

Zusätzlich können Sie folgende Boxcryptor-Einstellungen ändern:



Wir empfehlen nur **erfahrenen Nutzern** diese erweiterten Einstellungen zu verändern.

- **Windows Suche aktivieren:** Dem Windows Indizierungsdienst Zugriff auf das Boxcryptor Laufwerk gewähren. Mehr darüber finden Sie [hier](#).
- **Papierkorb aktivieren:** gelöschte Dateien werden in den Papierkorb verschoben, so dass Sie bei Bedarf wiederhergestellt werden können
- **Als Festplatte einbinden:** Das Boxcryptor Laufwerk ist ein virtuelles Laufwerk. Dennoch bindet diese Option es so ein, als wäre es ein reales Laufwerk.
- **Für alle Benutzer einbinden:** Systemkonten können Boxcryptor benutzen
- **Unterstützung für lange Pfade aktivieren** (nur in Windows 7|8|8.1): Aktiviert Dateipfade mit mehr als 256 Zeichen. Vorsicht: Es können Probleme mit anderen Programmen auftreten.



Boxcryptor übernimmt die systemweite (ab Windows 10 unterstützte) Einstellung: *Lange Win32-Pfade aktivieren*. [Hier](#) finden Sie eine Anleitung, um diese zu aktivieren.



Die Unterstützung für lange Pfade hängt von den Eigenschaften der zugrunde liegenden Dateisysteme ab. Ältere Dateisysteme wie FAT32 (normalerweise für USB-Sticks verwendet) können von dieser Einstellung *nicht* profitieren.

- **In Windows Mount Manager einbinden:** Fügt das Boxcryptor-Laufwerk im Windows Mount Manager hinzu.
- **Dateien und Ordner mit einem Punkt am Anfang verstecken:** Mit dieser Option wird das Verstecken dieser Dateien erzwungen.
- **Dateien und Ordner mit nicht entschlüsselbaren Namen ausblenden:** Wenn Dateien und Ordner nicht entschlüsselt werden können, haben Sie keinen Zugriff darauf. Deshalb blenden wir diese aus.
- **OneDrive Online-Dateiwarnung ausblenden:** Boxcryptor kann nicht mit den "on-demand" Dateien des in *Windows 8* integrierten OneDrive Clients umgehen. Aktivieren Sie diese Option um Fehlermeldungen zu verhindern, wenn Sie Ordner mit solchen Dateien durchsuchen. Die neuere Version des Clients sowie die Implementierung in Windows 10 wird unterstützt.
- **Automatische Erkennung von Wechseldatenträgern:** Automatisches Einbinden von USB-Sticks oder externen Laufwerken als Boxcryptor Speicherorte.
- **Automatische Erkennung von Netzlaufwerken:** Automatisches Einbinden von Netzlaufwerken als Boxcryptor-Speicherorte.

Boxcryptor-Konto

Ihr Konto verwalten

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

Passwort wiederherstellen

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



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

Sie können Ihr Konto [hier](#) zurücksetzen.

Geräte und Sitzungen verwalten

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

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

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

Schlüssel exportieren

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

Sie können Ihre Schlüssel exportieren, wenn Sie [sich auf unserer Webseite mit Ihrem Konto anmelden](#):

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



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

Lokales Konto

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

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


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



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

> Eine Schlüsseldatei exportieren

Eine bestehende Schlüsseldatei öffnen

1. Klicken Sie im Anmeldebildschirm auf .
2. Wählen Sie **Boxcryptor mit einem lokalen Konto nutzen**.
3. Wählen Sie Ihre Schlüsseldatei aus.
4. 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:

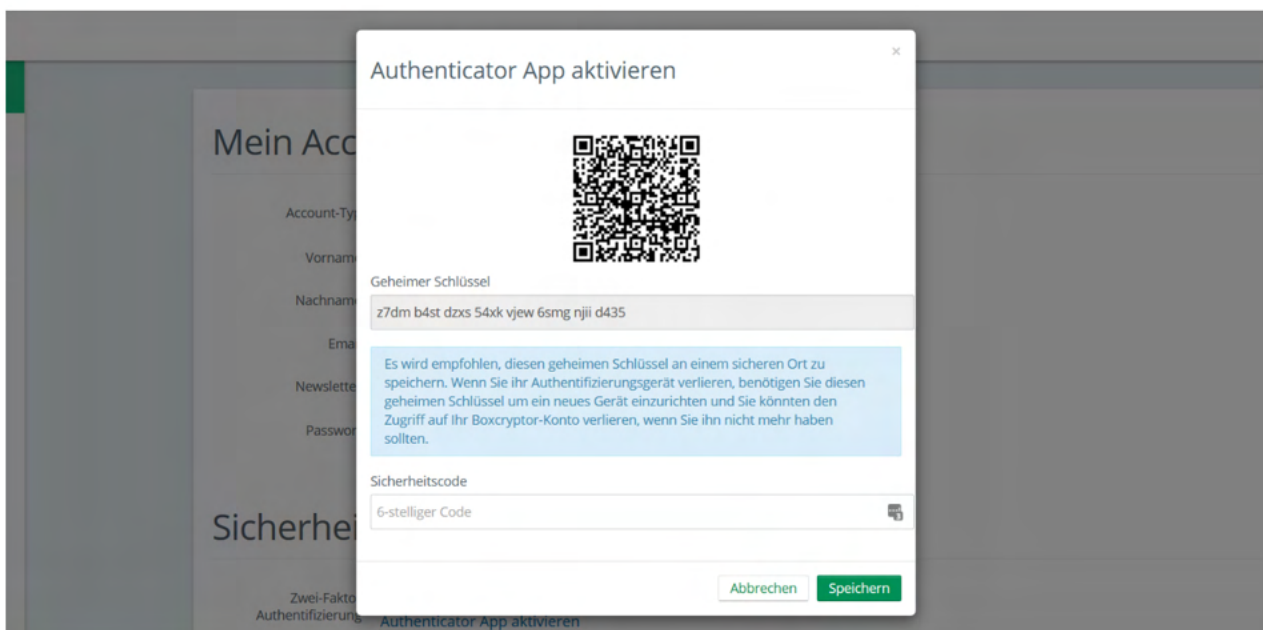
1. Melden Sie sich auf boxcryptor.com an.
2. Navigieren Sie zu **Sicherheit**.
3. Aktivieren Sie **Zwei-Faktor-Authentifizierung -> Authenticator-App**.

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](#)



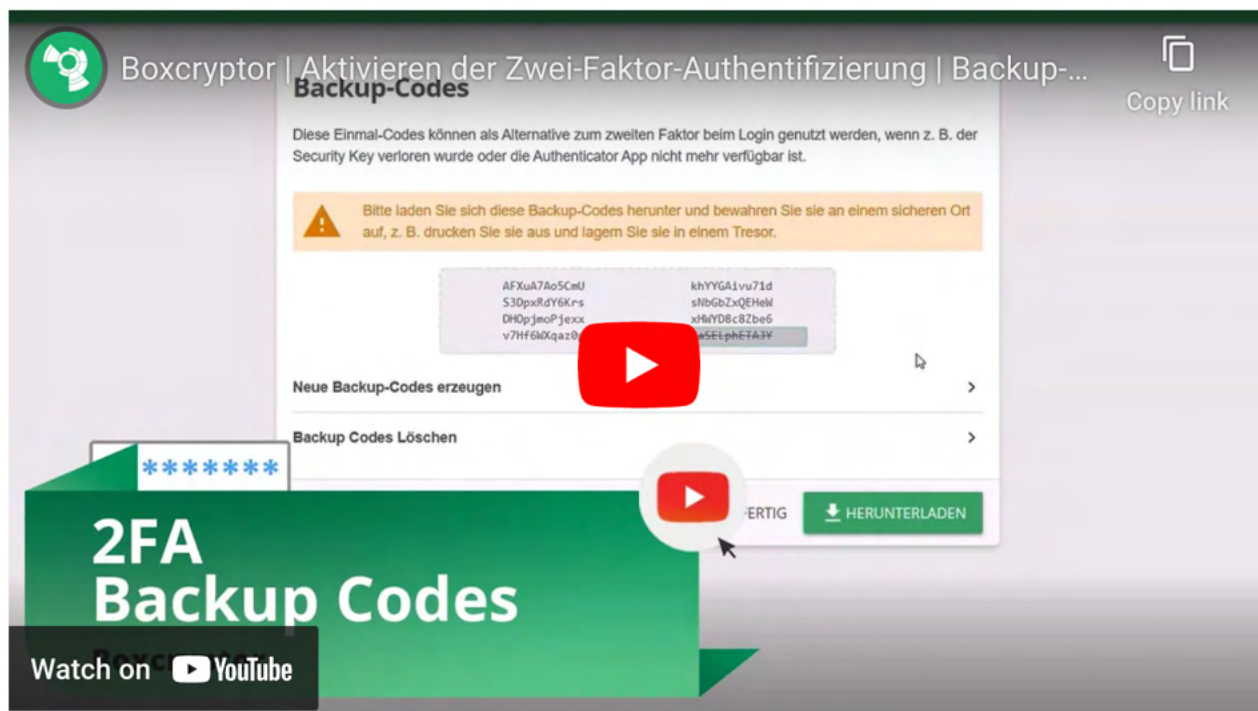
Um ein versehentliches Aussperren zu vermeiden empfehlen wir das Registrieren eines zweiten Security Keys. Nutzen Sie den Ersten für Ihre täglichen Geschäfte und bewahren Sie den Zweiten als Backup auf, falls Sie den ersten verlieren. Alternativ können Sie auch TOTP als zweiten Backup-Faktor einrichten.

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

Backup-Codes

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

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



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

2FA und die App-Schutz

2FA kommt nur bei Anmeldungen mit Ihrem Boxcryptor-Konto zum Einsatz. Wenn Sie bereits angemeldet sind, wird der zweite Faktor nicht weiter benötigt - selbst wenn Sie den [App-Schutz](#) aktiviert haben. Dieses Sicherheitsfeature hilft gegen unauthorisierten Zugriff auf Boxcryptor wenn Sie **bereits angemeldet sind**. Aus diesem Grunde werden Sie nicht nach Ihrem zweiten Faktor gefragt. Um sicherzustellen, dass Boxcryptor nach Ihrem zweiten Faktor fragt, müssen Sie sich zuerst komplett abmelden.

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

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

FAQ & Fehlerbehebung

Off-Migration Guide: Alle mit Boxcryptor verschlüsselten Dateien entschlüsseln

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

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



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

✓ Migration Tips für Unternehmen

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

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



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

Was passiert, wenn es Boxcryptor nicht mehr gibt?

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

möchten, dass die Boxcryptor Server dauerhaft offline sein sollten:

- Exportierte Schlüsseldatei
- Installationsdatei für Boxcryptor

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

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

Ich kann Boxcryptor nicht installieren

Wenn Sie Boxcryptor nicht installieren können, versuchen Sie folgende Schritte:

Sicherstellen, dass .NET korrekt installiert ist

- Installieren Sie [Microsoft .NET Framework Repair Tool](#) und folgen Sie den Anleitungen.
- Installieren Sie das neueste [.NET Framework](#).
- Starten Sie Ihr System neu.
- Installieren Sie Boxcryptor.

Installation als Administrator starten

Falls das nicht funktioniert, versuchen Sie, die Setup-Datei manuell mit einem Rechtsklick auf → **Als Administrator installieren** zu starten.



Diese Option wird nur angeboten, wenn das momentane Windows Benutzerprofil *kein* Administratorprofil ist.

Bekannte Installationsprobleme

Es gibt einige bekannte Installationsprobleme, für die wir derzeit an einer Lösung arbeiten:

✓ Fehlercode: 267

Während der Installationsroutine zeigt das Installationsprogramm **Fehlercode: 267**.

Das bedeutet, dass der Benutzerprofilordner und der darin enthaltene Ordner Temp von der Installationsroutine nicht gefunden werden können. Dies scheint mit einem vorhergegangenen Upgrade von Windows zusammenzuhängen.

Workaround

Installieren Sie Boxcryptor von einem **anderen Windows-Benutzerprofil**. Wenn kein anderes Benutzerkonto vorhanden ist, erstellen Sie [hier](#) vorübergehend eines. Anschließend kann das temporäre Profil gelöscht oder deaktiviert werden. Boxcryptor ist nun über das ursprüngliche Windows-Konto nutzbar.

✓ Missing DLL

Während des Installationsvorgangs zeigt Windows folgende Fehlermeldung:

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

Dies wird durch Antivirensoftware verursacht, welche Boxcryptor fälschlicherweise als schadhafte Software einstuft und daraufhin die Installation verhindert.

Workaround

Damit Boxcryptor korrekt installiert werden kann, stellen sie bitte sicher das keine Antivirensoftware in den Installationsprozess eingreifen kann. Hierzu können sie folgendes tun:

- Deaktivieren sie kurz ihren Virenschutz während des Installationsvorgangs
- Fügen sie ihrem Antivirenprogramm eine Ausnahmeregel für Boxcryptor hinzu
- Deinstallieren Sie Ihre Antivirensoftware und installieren Sie sie erneut, nachdem die Installation von Boxcryptor abgeschlossen ist

Falls die Installation weiterhin fehlschlägt

Falls dies auch nicht weiterhilft, benötigen wir mehr Feedback über den Installationsablauf:

- Drücken Sie den **Windows Key+R**, tippen Sie `cmd` und drücken danach **Enter**.
- Tippen Sie `cd <path to your installation file>` in dem neuen Fenster.
- Geben Sie nun `<installation file> /log log.txt` ein.

Dieser Befehl erstellt eine `log.txt` Datei im gleichen Verzeichnis, in dem Ihre Installationsdatei gespeichert ist und enthält wichtige Informationen über die fehlgeschlagene Installation. Lesen Sie die Datei durch, um den Grund für die fehlgeschlagene Installation zu finden oder [schicken Sie es uns](#).

Mein Bildschirm wird bei der Installation schwarz

Während der Installation müssen wir den Explorer stoppen, um die Kernel-Treiber-Integration zu

installieren. Manchmal kann der Microsoft Software Installer (msi) keine vorherigen Anwendungen wiederherstellen. In diesem Fall müssen Sie den Explorer neu starten.

- Öffnen Sie den Task-Manager (**Ctrl + Shift + Esc**).
- Klicken Sie auf **Datei** → **Neue Aufgabe**.
- Geben Sie "explorer" ein und drücken Sie Enter, um den Explorer-Prozess wiederherzustellen.

Ich kann Boxcryptor nicht aktualisieren oder entfernen

Gelegentlich schlägt eine Deinstallation oder ein Update von Boxcryptor fehl. In diesem Fall fordert Boxcryptor die originale Installationsdatei. Dieses Problem wird durch aggressive Systemverbesserungsprogramme ausgelöst.

Um dies zu beheben, **laden Sie einfach das Installationsprogramm für die aktuell installierte Boxcryptor-Version aus [unserem Change Log](#) herunter** und stellen es auf Nachfrage bereit.

Falls das nicht ausreicht, probieren Sie es mit [Microsoft's Deinstallations-Tool](#).

WebView2 Fehlerbehebung

Boxcryptor setzt für bestimmte Fälle wie die **Anmeldung** und die **Whispily-Integration** auf Microsofts **WebView2 (Evergreen) Laufzeit**.

Diese Laufzeit wird automatisch mit Windows 11 ausgeliefert, bei Windows 10-Installationen, die Microsoft-Technologien wie Microsoft 365 verwenden, ist die Laufzeit ebenfalls vorinstalliert.

Evergreen impliziert, dass Microsoft selbst dafür verantwortlich ist, die Laufzeit auf dem neuesten Stand zu halten, sodass Entwickler sicher sein können, dass die neuesten Funktionen und Sicherheitsfixes auf Client-Computern bereitgestellt werden, ohne ihre Apps aktualisieren zu müssen.

Es gibt jedoch Szenarien, in denen dieses automatische Update nicht wie erwartet funktioniert, was zu Versions- und Kompatibilitätsabweichungen zwischen dem WebView2-Modul der App und dem Laufzeit-Pendant führen kann.

Boxcryptor versucht, dieser Situation zu begegnen, indem „neuere“ Funktionen der Webansicht selektiv deaktiviert werden, um zumindest die Grundfunktionalität verfügbar zu halten.

Wir empfehlen jedoch **nicht**, Ihre WebView2-Laufzeit in diesem **veralteten Zustand zu belassen**. Folgende Ansätze gibt es, dieses Problem zu beheben:

✓ Installieren Sie die neuste Version

Microsoft stellt einen Downloader zur Verfügung, der Ihre WebView2-Laufzeit auf dem neuesten Stand halten sollte. Manchmal hilft es, ihn einfach erneut zu installieren. Sie können diesen [hier](#) herunterladen.

✓ Reparieren Sie Ihre aktuelle Installation

In einigen Fällen kam es vor, dass die Installation in einem beschädigten Zustand feststeckt. Um dies zu beheben, gehen Sie bitte zu Ihren [Apps und Funktionen](#), suchen Sie nach „Microsoft Edge WebView2 Laufzeit“ und wählen Sie „Ändern“ im 3-Punkt-Menü. Das Installationsprogramm wird nun mit der Option zum „Reparieren“ der aktuellen Installation angezeigt.

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 - z. B. Lesen oder Schreiben von Dateien -, steigt die CPU-Last. Finden keine Aktivitäten auf dem Boxcryptor-Laufwerk statt, sollte die CPU-Last gering sein.

Es ist jedoch **möglich, dass diese Aktivitäten nicht sichtbar sind**, z. B. wenn Applikationen Hintergrundaktivitäten ohne direkten Einfluss des Nutzers durchführen. Ein klassisches Beispiel hierzu sind Indexierungen des Windows Suchdienstes.

Boxcryptor ist langsam

Eine App ist langsamer als gewöhnlich bei der Nutzung mit Boxcryptor

Wenn sich eine App in Kombination mit Boxcryptor langsamer als gewöhnlich verhält, kann es daran liegen, dass die Applikation ein Problem mit der Verschlüsselung von Boxcryptor hat. Boxcryptor fungiert einfach als Filter, der Lese- und Schreibabfragen des Betriebssystems annimmt und sie dabei verschlüsselt.

Gut geschriebene Applikationen schreiben ihre Dateien in Blöcken. In diesem Fall muss Boxcryptor nur wenige Male während der Verschlüsselung aktiv werden und die Performance wird nicht beeinträchtigt. Einige Applikationen schreiben jedoch jedes Byte einzeln. Dies führt zu vielen Anfragen an Boxcryptor und führt zu reduzierter Performance.

Falls Sie Probleme mit einer Ihrer regelmäßig genutzten Apps haben und Ihre Priorität auf Performance liegt, können Sie eine Alternative ausprobieren, um zu prüfen, ob diese besser mit der Verschlüsselung von Boxcryptor umgehen kann.

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. Windows Suche.

Symbole oder das Kontextmenü werden nicht angezeigt

Boxcryptor verwendet für die Kommunikation mit dem Explorer seinen eigenen Kanal um Overlay-Symbole oder das Kontextmenü anzeigen zu lassen. Wenn keines von beiden angezeigt wird,

funktioniert diese Kommunikation höchstwahrscheinlich nicht. Es gibt hierfür drei mögliche Gründe:

Sie haben entweder Boxcryptor oder den Explorer als einen anderen Benutzer gestartet

Korrigieren Sie dies, indem Sie im Task Manager (**Strg+Shift+Esc**) zuerst **Boxcryptor** → Neustarten und dann **Explorer** → Neustarten wählen.

Es laufen zu viele Explorer-Prozesse gleichzeitig

Boxcryptor bearbeitet nur eine eingeschränkte Anzahl an Explorer-Prozessen gleichzeitig. Korrigieren Sie dies, indem Sie über den Task Manager (**Strg+Shift+Esc**) einige **Explorer-Instanzen** schließen.

Alle freien Plätze für die Overlay-Symbole sind belegt

Windows 10 hat diese auf 9 freie Plätze beschränkt, diese werden nun von allen installierten Programme 'umkämpft'. Bitte berücksichtigen Sie, dass jedes einzelne Symbol einen freien Platz benötigt.

Die Lösung ist, alle ungenutzten Einträge zu löschen: 1. Öffnen Sie die Registry: **Windows-Taste + R** → **regedit** eingeben → **EINGABE** drücken 2. Navigieren Sie zu diesem Schlüssel: **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers** 3. Löschen Sie alle Schlüssel die Ihrer Meinung nach nicht mehr benötigt werden oder "SkyDrive" ähneln. (SkyDrive ist das alte OneDrive.) 4. Starten Sie Ihr System neu.



Sie können gerne dabei helfen, Microsoft auf dieses Problem aufmerksam zu machen. "Voten" Sie dazu [hier](#) über den Microsoft Feedback Hub.

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
- Ereignisprotokolleinträge von Boxcryptor
- Benutzerinteraktion und Screenshots, die mit Windows Schrittaufzeichnung aufgezeichnet wurden

Wie erstelle ich ein Debug Log?

1. Gehen Sie zu Ihrem Boxcryptor-Installationsverzeichnis (C:\Program Files (x86)\Boxcryptor), → **Doppelklick auf Boxcryptor (Debug)**.
2. Wiederholen Sie alle Schritte, die zu dem unerwarteten Verhalten geführt haben.
3. Verlassen Sie Boxcryptor durch einen Rechtsklick auf das Symbol → **Exit**.

Ein Debug-Log-Archiv (Boxcryptor-<Zeitstempel>.seclog.zip) wird erzeugt und auf dem Desktop gespeichert.

✓ Zusätzliche Systeminformationen

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

1. Drücken Sie **Windows** → schreiben Sie `msinfo32` → drücken Sie **Eingabe**. Nun öffnet sich die Systeminformations-Übersicht.
2. Gehen Sie nun auf **Datei** → **speichern**, um die Informationen zu exportieren und uns zusätzlich zukommen zu lassen.

✓ Logging während Boxcryptor läuft

Sollten Sie auf ein Problem stoßen, zu dem Sie direkt ein Log erstellen wollen, können Sie auch im laufenden Betrieb von Boxcryptor das Logging aktivieren:

1. Drücken Sie **Windows-Taste+R** → schreiben Sie `bc.cmd` → drücken Sie **Eingabe**. Damit wird eine interaktive Boxcryptor-Konsole gestartet.
2. Geben Sie `debug` ein → drücken Sie **Eingabe**.
3. Wiederholen Sie alle Schritte, die zu dem Problem geführt haben.
4. Verlassen Sie Boxcryptor durch einen Rechtsklick auf das Symbol → **Beenden**, oder deaktivieren sie das Logging über die Konsole: `debug --set-debug-mode=FALSE`.

✓ Boxcryptor während des Hochfahrens von Windows loggen

1. Drücken Sie **Windows-Taste+R** → schreiben Sie `bc.cmd` → drücken Sie **Eingabe**. Damit wird eine interaktive Boxcryptor-Konsole gestartet.
2. Geben Sie `debug --persistent` ein → drücken Sie **Eingabe**, um das permanente

Loggen zu aktivieren.

3. Schliessen Sie anschließend das Fenster der Konsole.

Boxcryptor wird Sie beim Start von Windows an das Ausschalten erinnern.

✓ 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:

1. Drücken Sie **Windows-Taste+R** → schreiben Sie `bc.cmd` → drücken Sie **Eingabe**. Damit wird eine interaktive Boxcryptor-Konsole gestartet.
2. Geben Sie `debug --eager-logging` ein → drücken Sie **Eingabe**, um das vorzeitige Loggen zu aktivieren.
3. Schliessen Sie anschließend das Fenster der Konsole.

Windows Schrittaufzeichnung

Um besser zu verstehen, wie das Problem entstanden ist, verwenden wir die in Windows integrierte [Schrittaufzeichnung](#). Dieses macht Screenshots, zeichnet Mausklicks auf und erkennt Tastatureingaben.



Sie werden eine leichte Leistungsminderung spüren, während die Schrittaufzeichnung läuft.

Microsofts Schrittaufzeichnung wird **keinerlei** Tastatureingaben aufzeichnen (es markiert lediglich Eingaben als Tastatureingabe). Solange Sie ihre Passwörter in Passworteingabefelder tippen (die die Eingabe verschleiern), werden Sie auch in den Screenshots nicht angezeigt.

Um sicherzustellen, dass alles nach Ihren Wünschen aufgenommen wurde, können Sie die Schrittaufzeichnung öffnen und überprüfen (`Boxcryptor-<Zeitstempel>.seclog.zip\<Zeitstempel>-steps-recorder.zip\Recording_<Zeitstempel>.mht`), bevor Sie uns das Protokoll senden.

✓ Schrittaufzeichnung deaktivieren

Wenn Sie keine Benutzerinteraktion aufgezeichnet haben möchten, können Sie entweder die Schrittaufzeichnung aus der .zip Datei löschen oder den Debug-Modus ohne Schrittaufzeichnung wie folgt starten:

Drücken Sie **Windows Key + R** → Geben Sie `bc.cmd` ein → Drücken Sie **Eingabe**. Dies öffnet eine interaktive Boxcryptor-Konsole. 2. Geben Sie `debug --disable-steps-recorder` ein → Drücken Sie **Eingabe**. 3. Schließen Sie anschließend das Konsolenfenster.

Was soll ich mit meinem Debug Informationen tun?

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

Boxcryptor stürzt beim Start ab

Wenn Boxcryptor beim Start der Software abstürzt, ist es wahrscheinlich, dass einige Komponenten der Installation fehlerhaft sind. Um dies zu beheben, versuchen Sie folgende Schritte:

- Deinstallation von Boxcryptor.
- Installation des [.NET-repairtool](#).
- Installation des aktuellsten [.NET framework](#).
- Neustart des Systems.
- Erneute Installation von Boxcryptor.

✓ Probleme unter Windows 7

Boxcryptor erfordert einige Komponenten, die möglicherweise fehlen, wenn **automatische Windows-Updates deaktiviert** sind.

Aktivieren Sie die automatischen Windows-Updates (empfohlen) oder laden Sie [KB2999226](#) manuell herunter und installieren Sie es.

Weitere Informationen zu diesem Update finden Sie [hier](#).

Ich kann mich nicht mit den Boxcryptor-Servern verbinden

Je nach System oder Netzwerkkonfiguration kann Boxcryptor sich möglicherweise nicht mit unseren Servern verbinden. Es gibt jedoch für die nachfolgend aufgeführten Meldungen einige Lösungsmöglichkeiten.

Nach der Anmeldung kehrt die App einfach zum Anmeldebildschirm zurück

Dies kann auf falsch konfigurierte SSL / TLS-Einstellungen zurückzuführen sein. Boxcryptor benötigt **TLS 1.2 oder höher** für eine sichere Client-Server-Kommunikation. Unter Windows 7 oder einigen falsch konfigurierten Computern ist TLS 1.2 möglicherweise nicht aktiviert.

Schauen Sie sich diese [Microsoft-Dokumentation](#) zum Aktivieren von TLS 1.2 an. Die bequemste Art, dieses Problem zu beheben, ist der in der Dokumentation verlinkte [Einfache Korrektur Installer](#).



In seltenen Fällen werden kritische [.NET-Updates](#) nicht auf Windows 7-Computern installiert, die höchstwahrscheinlich Verbindungsprobleme selbst bei aktivierter TLS 1.2-Unterstützung verursachen. Microsoft bietet zu jedem Update einige Tipps zur Fehlerbehebung auf den jeweiligen Landingpages an.

Warnung: Dies ist keine sichere Verbindung

Wenn in Ihrer Systemumgebung der **Datenverkehr** überwacht wird, ist es möglich, dass eine Verbindung zu unseren Servern verhindert wird. Beispiele, bei denen die Überwachung des Datenverkehrs zu Problemen mit Boxcryptor führt:

- Anti-Virus-Lösungen, die den Datenverkehr mit dem Internet überwachen
- Öffentliche Hotspots
- Proxy-Server des Unternehmens
- **Malware**

Datenverkehrsüberwachung ist technisch gesehen ein **Man-in-the-Middle-Angriff**. Es ist daher wichtig, dass Ihr System nicht gefährdet ist.

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.

Proxy-Unterstützung

Boxcryptor übernimmt die [Proxy-Einstellungen für Windows](#), einschließlich authentifizierter Proxies (die bei Bedarf authentifiziert werden).

Falls Boxcryptor Ihre Proxy-Konfiguration umgehen soll, fügen folgende Regeln zur Ausschlussliste hinzu:

```
*.boxcryptor.com // für Zugriff auf die API (erforderlich)
*.secomba.com // für Update-Prüfungen (optional)
```

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 Betriebssystemen.

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 Windows hier herunter:

https://www.boxcryptor.com/download/Boxcryptor_Classic_v1.7.409.131_Setup.msi *Unterstützt Windows XP, Windows 7, Windows 8.1*

Laden Sie Boxcryptor Classic Portable für Windows hier herunter:

https://www.boxcryptor.com/download/BoxcryptorClassicPortable_1.6.402.92.zip *Unterstützt Windows XP, Windows 7, Windows 8.1*

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.

So verwalten Sie die Anwendungskonfigurationsdatei

Die Boxcryptor-Konfigurationsdatei **Boxcryptor.exe.config** befindet sich im Installationsordner von Boxcryptor (**%PROGRAMFILES(x86)%\Boxcryptor**). Um Änderungen an dieser Datei vorzunehmen, öffnen Sie diese in einem Texteditor.



Änderungen in **%PROGRAMFILES(x86)%** erfordern Administratorrechte. Wenn Sie den Standard-Texteditor (**Notepad.exe**) verwenden, muss dieser als Administrator ausgeführt werden, um Änderungen erfolgreich zu speichern. (**Windows Key** + "Notepad" eingeben -> Rechtsklick auf den Texteditor im Suchergebnis -> **Als Administrator ausführen**)

Stellen Sie außerdem sicher, dass das Ergebnis als ".config" - Datei gespeichert wird, da einige Editoren möglicherweise noch ".txt" anhängen.

Die Anwendungskonfigurationsdatei ist eine XML-basierte Konfiguration mit folgendem Format:

```
<configuration>
...
<appSettings>
  <add key="SCHLÜSSEL" value="WERT" />
</appSettings>
...
</configuration>
```

Um eine Einstellung zu ändern, die durch **key** definiert ist, ändern Sie die zugehörige Zeichenfolge unter **value**.



Die Konfigurationsdatei wird beim Starten von Boxcryptor geladen. Wenn Boxcryptor beim Ändern der Konfiguration ausgeführt wird, müssen Sie Boxcryptor neu starten, damit die Änderung wirksam wird.



Durch das Aktualisieren von Boxcryptor wird möglicherweise die Konfigurationsdatei zurückgesetzt. Stellen Sie sicher, dass Sie eine Sicherungskopie Ihrer Konfiguration erstellen.

Liste der Anwendungseinstellungen

- **EncryptByDefault** (Standard **false**): Neue Dateien, die von Anwendungen in unverschlüsselten Verzeichnissen erstellt wurden, werden standardmäßig verschlüsselt geschrieben.
- **AlternateDataStreamSupport** (Standard **true**): Unterstützung für alternative Datenströme. Beachten Sie, dass die ADS-Unterstützung nur aktiviert ist, wenn alle aktivierten Boxcryptor-

Speicherorte diese Funktion unterstützen.

- **EncryptDialogIncludedProcesses:** Eine durch Kommas getrennte Liste von Prozessen, die den Dialog "Möchten Sie diese Datei verschlüsseln" auslösen, wenn Sie Dateien bzw Ordner in unverschlüsselten Verzeichnissen erstellen.
- **SupportedBackupProcesses:** Eine durch Kommas getrennte Liste von Prozessen, die Backup-optimierte Dateisystem-E/A erhalten wie z. B. das frühzeitige Herunterladen von On-Demand-Dateien.
- **CreateLogOnCrash** (Standard `true`): Erzeugung einer Log Datei unter `%LOCALAPPDATA%\Boxcryptor\Crash Logs` nach einem App-Absturz.
- **ProcessNamesPreventingShutdownOnSessionEnd:** Eine durch Kommas getrennte Liste aller Prozesse, die geschlossen werden müssen, bevor Boxcryptor am Ende der Sitzung geschlossen wird. Dies dient dazu Datenverlust bei Dateien zu vermeiden, die über das Boxcryptor-Volume geöffnet wurden.
- **DisableAutomaticUpdates** (Standard `false`): Verhindert automatische Updates und unterdrückt auch alle Update-Benachrichtigungen.
- **DisableExplorerQuickAccess** (Standard `false`): Deaktiviert die Erstellung des Boxcryptor-Schnellzugriffssymbols im Navigationsbereich des Windows-Explorers.
- **CustomSettingsPath** (Standard `""`): Ein benutzerdefinierter Pfad, in dem Boxcryptor die Benutzereinstellungen speichert. Kann Umgebungsvariablen enthalten. Weitere Informationen finden Sie unter [Teams/Deployment/Speicherort für benutzerdefinierte Einstellungen](#).
- **EnableTerminalEnvironmentMode** (Standard `false`): Definiert und beschränkt bestimmte Boxcryptor-Einstellungen so, dass sie mit Thin Clients (Terminal / Citrix Server) kompatibel sind.
- **RefreshUserPeriodMs** (Standard `15000`): Definiert den Zeitraum in Millisekunden, in dem sich der Client mit den Boxcryptor-Servern synchronisiert.
- **DisableInitialTutorialAndTour** (Standard `false`) Deaktiviert dauerhaft die automatische Anzeige des Tutorials und der Einführung.
- **WebView2CommandLineParameters** (Standard `""`): Bietet die Möglichkeit, Befehlszeilenparameter an die WebView2 Web-Rendering-Engine zu übertragen.
- **TryReconnectRemoteLocationsOnStartup** (Standard `true`) Versucht, die Verbindung zu nicht verbundenen Netzwerkspeicherorten (SMB und WebDAV) beim Start wiederherzustellen. Zeigt möglicherweise einen Benutzerauthentifizierungsdialog an.

Veraltete Versionen

Wir veröffentlichen regelmäßig neue Versionen von Boxcryptor mit neuen Features, besserer Stabilität und allgemeinen Verbesserungen und stellen veraltete Versionen in regelmäßigen 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*.

Windows Suche / Cortana verwenden

Um die Windows Suche bzw. Cortana für das Suchen in Boxcryptor-verschlüsselten Dateien verwenden zu können, sind folgende [erweiterte Einstellungen](#) erforderlich:

- Windows Suche aktivieren
- Als Festplatte einbinden
- Für alle Benutzer einbinden
- In Windows Mount Manager einbinden

Anschließend muss das Boxcryptor Laufwerk in den Windows Indizierungsoptionen als Ort aufgenommen werden.



Manchmal erfordert das Ändern der Einstellungen einen **Neustart des Computers**, damit das Boxcryptor-Laufwerk als verfügbarer Speicherort in den Indizierungsoptionen angezeigt wird.



Das Hinzufügen des Boxcryptor-Laufwerks zum Windows-Suchindex kann zu einer erheblichen CPU-Auslastung und zu Leistungseinbußen führen, da Windows alle Dateien im Boxcryptor-Laufwerk indiziert. Darüber hinaus können Inhalte, die eigentlich verschlüsselt sind, im unverschlüsselten Windows-Suchindex landen.

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.

Inkompatibilität mit Bitdefender

Wir haben in letzter Zeit gehäuft Kundenfeedback erhalten, dass das Boxcryptor Laufwerk nach einigen Stunden Betrieb oder nach dem Standby des Systems nicht mehr verfügbar ist bzw. Boxcryptor selbst nicht mehr läuft.

In der [Windows Ereignisanzeige](#) → [Windows-Protokolle](#) → [Anwendung](#) werden diese Abstürze als Application Error folgendermaßen aufgeführt:

```
Name der fehlerhaften Anwendung: Boxcryptor.exe, Version: 2.XX.XXXX.0, Zeits  
Name des fehlerhaften Moduls: KERNELBASE.dll, Version: XX.XX.XX.XX, Zeitstem  
Ausnahmecode: 0xe0000008 | 0xe0434352  
[...]
```

Alternativ können auch unter .NetRuntime Fehler über System.OutOfMemoryException aufgeführt sein.

Ein weiterer Hinweis auf diesen Absturz ist ein **rotes Boxcryptor Symbol in der Systemleiste** und eine SSL-Benachrichtigung.

Nach einiger intensiver Recherche und Auswertung verschiedenster Fehlerlogs haben wir **Bitdefender** als den Verursacher des Problems identifizieren können.

Mögliche Workarounds

✓ Bitdefender für Zuhause

Abhilfe schafft hier vorerst nur Boxcryptor im Falle eines Absturzes neuzustarten , **Advanced Thread Defense** in Bitdefender zu deaktivieren oder **Bitdefender** zu **deinstallieren** und das System neuzustarten. Achten Sie hierbei darauf, dass Bitdefender möglicherweise mehrere einzelne Softwarekomponenten installiert.

✓ Bitdefender für Unternehmen

In Bitdefender Unternehmenslösungen (z.B. Gravity Zone) gibt es Optionen zum Hinzufügen von Boxcryptor.exe zu einer Ausnahmeliste für verschiedene Module (On-Demand, On-Access, ATC/IDS und Ransomware).

Wir haben bereits Bitdefender kontaktiert und werden die neusten Ergebnisse hier, sowie auch in unserer [Community](#) veröffentlichen.

Account Zugriff bei verlorenem zweiten Faktor (2FA) wiederherstellen

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

Möglichkeiten, den Zugriff auf Ihr Konto wiederherzustellen:

✓ Den geheimen Schlüssel aus der Ersteinrichtung erneut anwenden

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

Als Referenz sieht der geheime Schlüssel ähnlich aus wie:

| mzwe wocd mj3d qr3f njjw g2cm grqw cvli

✓ Einen Gerätecode verwenden

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

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



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

✓ Einen Backup-Code einsetzen

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



Sollten Ihnen die Einmalcodes ausgehen, können Sie [hier](#) neue Codes generieren.

✓ Keine der oben genannten Methoden sind möglich

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

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

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

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

Um einen Termin auszuwählen, gehen Sie bitte auf unsere [Buchungsseite](#).

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

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

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

Ungültige Codes der Authenticator App

Sollten Sie trotz funktionierender Authenticator App keine gültigen Codes generieren können, liegt

dies höchstwahrscheinlich an einer abweichenden Urzeit auf einem der beteiligten Systeme.

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

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

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

Sonstiges

Wartungsfenster

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

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

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

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

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

Changelog

Version 2.55.2774 (2022-11-08)

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

Version 2.54.2765 (2022-11-02)

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

Version 2.53.2568 (2022-07-27)

- Fixed: Incompatibility with Volume Shadow Copy Service (VSS)

- Fixed: File handles are closed with significant delay
- Changed: Plaintext files and folders no longer show a white overlay icon
- Changed: Upgraded CBFS Connect to v20.0.8181
- Minor bug fixes and improvements

Version 2.52.2484 (2022-05-27)

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

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

Version 2.51.2468 (2022-05-19)

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



This update requires a computer reboot

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

Version 2.50.2196 (2022-01-31)

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



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

Version 2.49.1965 (2021-10-14)

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

Version 2.48.1906 (2021-09-22)

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

Version 2.47.1752 (2021-06-30)

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

Version 2.46.1654 (2021-05-31)

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

Version 2.45.1556 (2021-03-29)

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



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

Version 2.44.1485 (2021-02-23)

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

Version 2.43.1441 (2021-02-03)

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

Version 2.42.1333 (2020-12-10)

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

Version 2.41.1246 (2020-10-07)

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

Version 2.40.1216 (2020-06-04)

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



This update requires a computer reboot

Version 2.39.1135 (2020-04-16)

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

Version 2.38.1080 (2020-02-10)

- Added: More folder icons for providers

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



This update requires a computer reboot

Version 2.37.1057 (2019-10-24)

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

Version 2.36.1046 (2019-09-02)

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

Version 2.35.1033 (2019-06-24)

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

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



This update requires a computer reboot

Version 2.34.995 (2019-03-20)

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

Version 2.33.933 (2019-01-25)

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

Version 2.32.910 (2018-12-10)

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

Version 2.31.870 (2018-10-19)

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

- Minor bug fixes and improvements



This update requires a computer reboot

Version 2.30.833 (2018-08-16)

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

Version 2.29.799 (2018-05-24)

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

Version 2.28.797 (2018-05-09)

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

Version 2.27.795 (2018-05-04)

- Updated: Privacy Policy
- Minor bug fixes and improvements

Version 2.26.784 (2018-04-23)

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

Version 2.25.777 (2018-04-06)

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

Version 2.24.747 (2018-02-28)

- Added: Downloading multiple on-demand files
- Fixed: Opening files can fail with Google Drive File Stream version 25.157.165.2150 and newer
- Fixed: Cannot copy files with alternate data streams to a location in the Boxcryptor drive which resides on a volume with does not support alternate data streams. The Boxcryptor drive only advertises alternate data stream support if all enabled locations reside on volumes with alternate data stream support (e.g. NTFS file systems)
- Minor bug fixes and improvements

Version 2.23.726 (2018-02-13)

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

Version 2.22.706 (2017-12-13)

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

Version 2.21.691 (2017-12-04)

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

Version 2.20.680 (2017-11-22)

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

Version 2.19.658 (2017-10-10)

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

Version 2.18.646 (2017-09-21)

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

Version 2.17.635 (2017-08-07)

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

Version 2.16.629 (2017-08-01)

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

Version 2.15.578 (2017-06-13)

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

Version 2.14.564 (2017-05-12)

- Improved: App stability
- Minor bug fixes and improvements

Version 2.13.560 (2017-05-06)

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

Version 2.12.553 (2017-04-24)

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

Version 2.11.550 (2017-04-18)

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

Version 2.10.542 (2017-04-04)



Likewise to Boxcryptor for macOS, Boxcryptor permissions are not checked when browsing into encrypted folders anymore. When any action is performed in an encrypted folder, permission checks still apply.

Checking permissions when browsing into an encrypted folder was only a "convenience" feature because the user could always browse into the folder directly in the location and the new behavior reflects this possibility also in the Boxcryptor drive.

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

Version 2.9.526 (2017-03-09)

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

Version 2.8.505 (2017-02-09)

- Minor bug fixes and improvements

Version 2.7.503 (2017-02-06)

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

Version 2.6.493 (2017-01-16)

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

Version 2.5.484 (2016-12-20)



Windows 7 users need the .NET Framework 4.5.2 to get Boxcryptor to run. You may find the download [here](#).

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



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

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

Version 2.3.415.455 (2016-09-26)

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

Version 2.3.413.448 (2016-09-08)

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

Version 2.3.411.446 (2016-09-01)

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

Version 2.3.409.438 (2016-08-25)

- Added: Command Line option to change default settings path
- Added: Duplicate file hiding resolving

- Files and folders hiding other items can now be automatically renamed.
- Added: Warning for bad encryption / decryption workflow
- Users will now be informed when they decrypt and re-encrypt folders unnecessarily
- Fixed: Encryption forbidden dialog could not be closed
- Fixed: Settings could get resetted when USB thumbsticks were removed
- Minor improvements and bug fixes

Version 2.3.407.426 (2016-08-09)

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

Version 2.3.405.406 (2016-07-27)

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

Version 2.3.403.402 (2016-07-21)

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

Version 2.3.401.400 (2016-07-07)

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

Version 2.2.423.322 (2016-04-04)

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



They are not actively supported by Microsoft anymore and we strongly encourage every user who is still using any of these old, unsecure operating systems to upgrade to a newer, secure version.

Version 2.2.421.309 (2016-03-09)

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

Version 2.2.419.277 (2016-02-23)

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

Version 2.2.417.266 (2016-02-03)

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

Version 2.2.415.246 (2015-12-22)

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

Version 2.2.413.244 (2015-12-16)

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

Version 2.2.411.228 (2015-10-19)

- Fixed: Minor bug fixes

Version 2.2.409.226 (2015-10-14)

- Added: Auto-detection for CudaDrive

- Fixed: Driver incompatibility with Strato HiDrive (and other CBFS-based drives).

Version 2.2.407.225 (2015-10-07)

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

Version 2.2.405.221 (2015-09-28)

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

Version 2.2.403.216 (2015-08-28)

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

Version 2.2.401.210 (2015-08-18)

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

Version 2.1.417.123 (2015-06-29)

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

Version 2.1.415.120 (2015-06-24)

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

Version 2.1.413.111 (2015-05-28)

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

Version 2.1.409.104 (2015-05-11)

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

Version 2.1.407.99 (2015-04-07)

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

Version 2.1.405.86 (2015-03-24)

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

Version 2.1.403.78 (2015-03-15)

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

Version 2.1.401.69 (2015-02-26)

- Added: Auto-detection for Dropbox for Business and other providers with multiple sync folders
- Added: Auto-detection for new storage providers (e.g. OneDrive for Business, Strato HiDrive, iCloud Drive, CloudMe, Cubby, Web.de, TelekomCloud, Storegate, SpiderOak, and SafeSync)

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

Version 2.0.437.408 (2014-10-27)

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

Version 2.0.435.407 (2014-09-15)

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

Version 2.0.433.406 (2014-09-02)

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

Version 2.0.431.403 (2014-08-06)

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

Version 2.0.429.396 (2014-07-11)

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

Version 2.0.427.395 (2014-06-30)

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

Version 2.0.425.394 (2014-06-23)

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

Version 2.0.423.392 (2014-06-16)

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

Version 2.0.421.388 (2014-06-11)

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

Version 2.0.419.376 (2014-04-10)

- Added: OneDrive for Business support

Version 2.0.417.367 (2014-02-24)

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

Version 2.0.415.357 (2014-02-20)

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

Version 2.0.413.343 (2013-12-19)

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

Version 2.0.411.330 (2013-11-07)

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

Version 2.0.409.325 (2013-11-07)

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

- Mount Manager" and "Mount For all Users")
- Minor bug fixes and improvements

Version 2.0.407.311 (2013-10-15)

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

Version 2.0.405.295 (2013-09-24)

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

Version 2.0.403.275 (2013-08-26)

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

Version 2.0.403.272 (2013-08-26)

- Changed: Fallback for opening pipe without elevated rights

Version 2.0.403.269 (2013-08-26)

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

Explorer++, Far Manager, FreeComander, SpeedComander, Total Commander, TeraCopy, xplorer2, XYplorer)

Version 2.0.402.252 (2013-08-09)

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

Version 2.0.401.229 (2013-07-23)

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

Version 2.0.401.172 (2013-06-28)

- Fixed: Installer not installing Callback FileSystem

Version 2.0.401.170 (2013-06-27)

- Fixed: Uninstaller crashing

Version 2.0.400.166 (2013-06-25)

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

Version 2.0.400.153 (2013-06-20)

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

Version 2.0.400.146 (2013-06-17)

- Removed context-menu placeholder for "Decrypt"

Version 2.0.400.145 (2013-06-15)

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

Version 2.0.400.138 (2013-06-14)

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

Version 2.0.400.121 (2013-06-07)

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

Version 2.0.400.116 (2013-06-05)

- Initial release

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](#)