

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 iOS 14. Boxcryptor für iOS ist mit dem iPhone, iPad und dem iPod Touch kompatibel.

Um Boxcryptor zu installieren, laden Sie die Boxcryptor-App aus dem [App Store](#) herunter.



Auf iOS-Geräten müssen Sie die App Ihres Cloud-Anbieters nicht installieren, da sich Boxcryptor direkt mit Ihrem Cloud-Anbieter verbindet. Wenn Sie die App Ihres Anbieters schon auf Ihrem Gerät installiert haben, können Sie diese einfach löschen, sobald Sie Boxcryptor eingerichtet haben.

Ein Boxcryptor-Konto erstellen



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

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

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

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



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



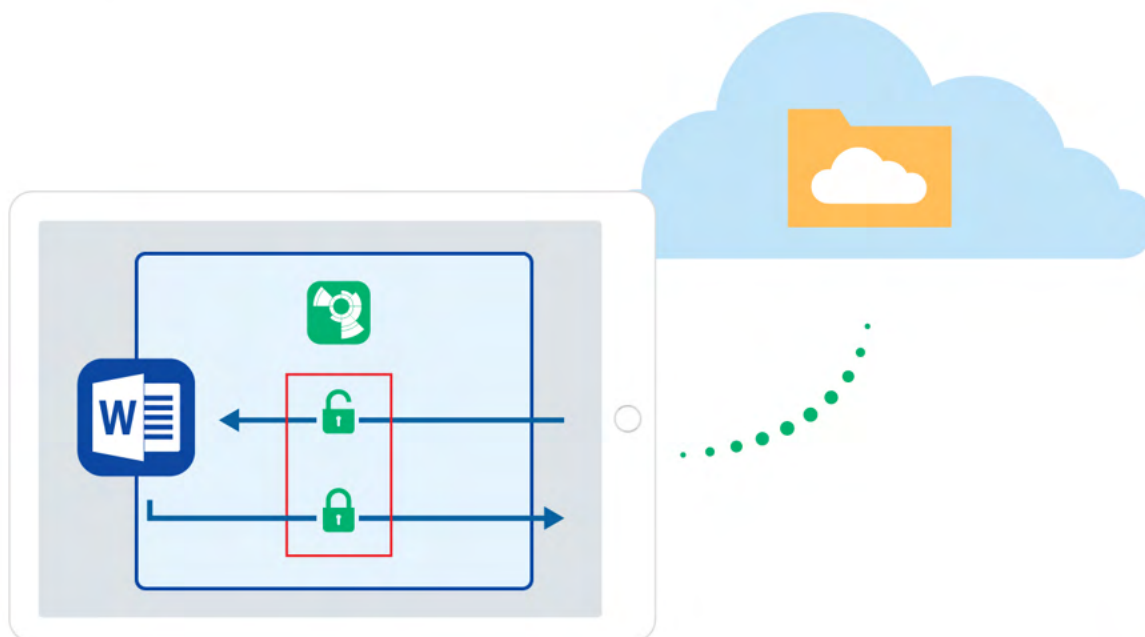
Aufgrund von Einschränkungen von Apple ist es nicht möglich, ein Boxcryptor-Konto innerhalb der iOS-App zu erstellen. Bevor Sie Boxcryptor für iOS verwenden, müssen Sie zuerst auf unserer Webseite [Ihr Konto erstellen](#).

Entdecken Sie Boxcryptor

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

können Sie Ihren [Cloud-Anbieter](#) hinzufügen und auf Ihre Dateien zugreifen.

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



Tags markieren Dateien und zeigen Ihnen, ob eine Datei oder ein Ordner verschlüsselt ist. ●.

Sie können Boxcryptor direkt aus anderen Apps heraus über die **Dateien-App-Integration** nutzen, beispielsweise in Word oder Pages.

Wie man bestehende Dateien verschlüsselt

Das Verschlüsseln von bereits existierenden Dateien ist mit Boxcryptor für iOS nicht möglich. Bitte verwenden Sie [Boxcryptor für Windows](#), [Boxcryptor für macOS](#) oder [Boxcryptor Portable](#), um Ihre bestehenden Dateien zu migrieren.

Verwalten Sie Ihre Clouds und Speicherorte

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

Speicherort hinzufügen

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

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



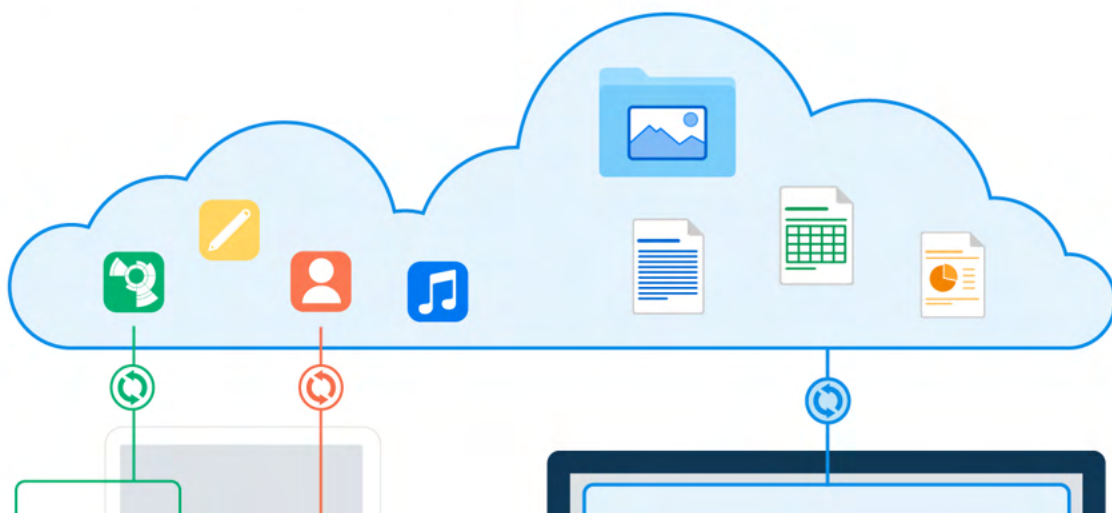
Sie können Ihren Provider auch durch langes Drücken **umbenennen** oder **löschen**.

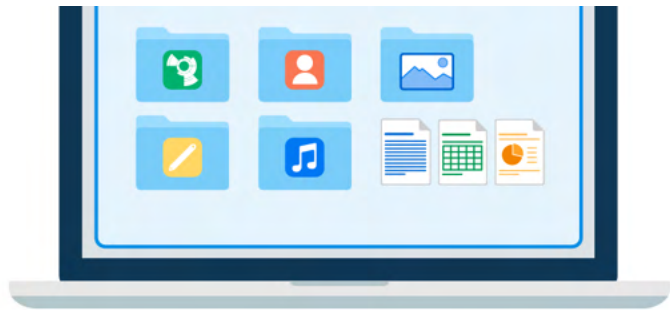
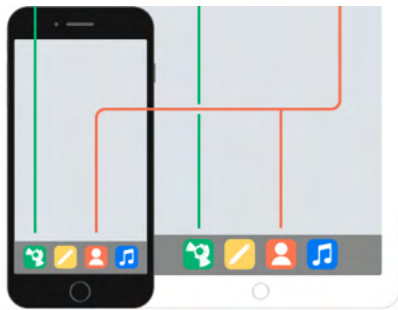
Google Drive

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

iCloud

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





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

WebDAV-Speicherorte

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

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



Boxcryptor erfordert eine gesicherte Server-Verbindung (<https://>) mit einem gültigen bzw. auf dem Gerät installiertem [selbst-signiertem SSL Zertifikat](#).

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

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



[ownCloud](#) und [nextCloud](#) unterstützen WebDAV. Standardmäßig lauten die Konfigurations-URLs:

<https://example.com/owncloud/remote.php/webdav>

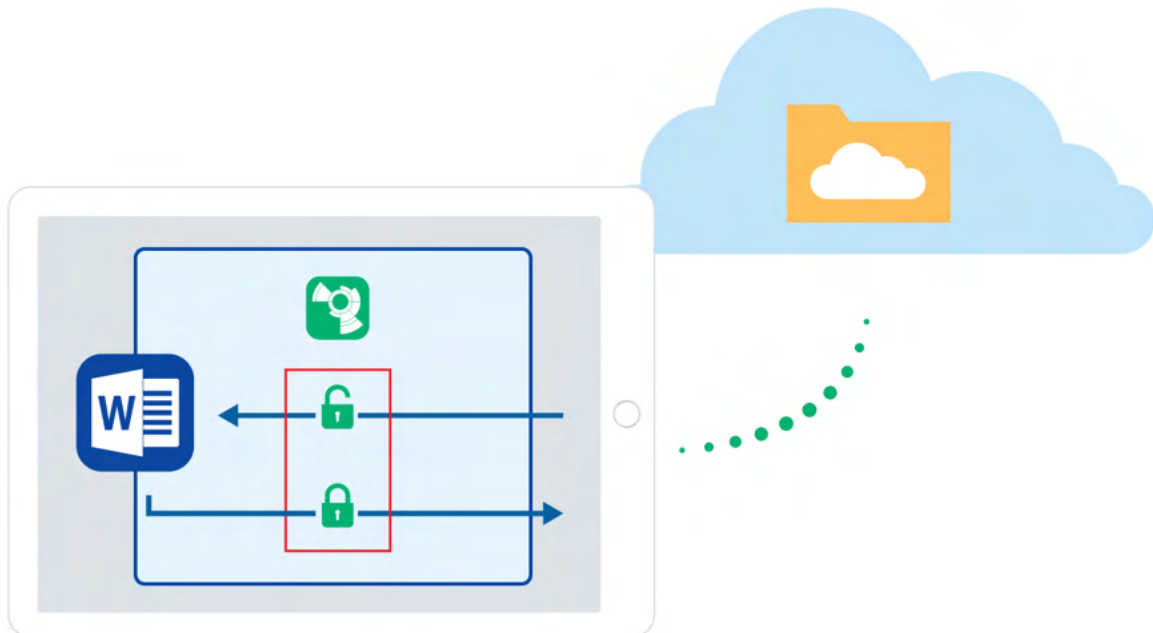
<https://example.com/nextcloud/remote.php/dav/files/username/>

Mit Dateien arbeiten

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

On-the-Fly-Verschlüsselung

Boxcryptor verschlüsselt Ihre Daten **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.



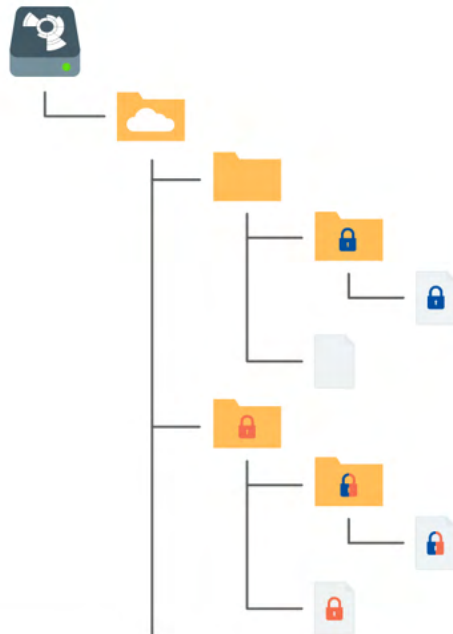
Wir entschlüsseln und verschlüsseln Ihre Dateien On-Demand: Sie wollen Ihre Inhalte sehen? Klicken Sie nur darauf und wir laden Ihre Datei für Sie herunter und entschlüsseln diese. Haben Sie Ihren Essay fertiggestellt? Senden Sie es einfach an Boxcryptor und wir verschlüsseln die Datei und speichern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

Verschlüsselungs- und Berechtigungshierarchie

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

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

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



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

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

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

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

Mit Ihren Dateien arbeiten

Mit Boxcryptor müssen Sie **Dateien nicht manuell entschlüsseln** um damit zu arbeiten. Die **Boxcryptor-Integration in die Dateien-App** lässt Sie in Ordner navigieren oder die Vorschau von Dateien ansehen, indem Sie darauf tippen. Boxcryptor wird **Dateien automatisch für Sie herunterladen und entschlüsseln**.

Funktionen innerhalb der Dateien-App

Mit Boxcryptor in der Dateien-App können Sie:

- Dateien, die mit Boxcryptor verschlüsselt sind, editieren und speichern.
- Dateien per Drag & Drop verschieben.
- Operationen an mehreren Dateien gleichzeitig ausführen.
- Erweiterte Sortieroptionen nutzen (Name, Datum, Größe, Tags).
- Bereits heruntergeladene Dateien in der Vorschau ansehen.
- Inhalte anderer Cloud-Anbieter einsehen, die noch keine Integration in die Dateien-App haben.

Mehr Funktionen der Dateien-App finden Sie in Apples eigener [Dokumentation](#).

Aktuelle Einschränkungen

- Neue Dateien und Ordner **erben** den Verschlüsselungsstatus des übergeordneten Verzeichnisses.
- Neue Dateien und Ordner werden **immer verschlüsselt**.

Wie Sie verschlüsselte Dateien erkennen

Boxcryptor ermöglicht es Ihnen, **verschlüsselte und unverschlüsselte** Dateien und Ordner im gleichen Verzeichnis zu verwalten. Innerhalb der Dateien-App wird der Verschlüsselungszustand mit Hilfe von **Tags** dargestellt:

-  **verschlüssel**
-  **unbekannt**
- Ohne Tag: **unverschlüssel**



Erst beim initialen Browsen in einen Ordner wird dessen Verschlüsselungszustand ermittelt.

Verschlüsselung vorhandener Dateien und Ordner

Das Verschlüsseln bereits vorhandener Dateien ist derzeit nicht möglich mit Boxcryptor für iOS. Benutzen Sie bitte [Boxcryptor für Windows](#), [Boxcryptor für macOS](#) oder [Boxcryptor Portable](#) zur Migration Ihrer existierenden Dateien.

Mit Dateinamenverschlüsselung arbeiten

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



Eine mit Dateinamenverschlüsselung versehene Datei sieht so aus: 恂惊掇抱峇珍殍相瞻 擗馊漢快搬濂檬湫惶掇挾柜樛秘.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, öffnen Sie die **Boxcryptor App**, navigieren Sie zu **Einstellungen** und wählen Sie **Dateinamenverschlüsselung aktivieren**.



Bereits vorhandene Dateien ohne Dateinamenverschlüsselung werden nicht geändert. Bitte benutzen Sie dafür die Desktop-Programme, dort können Sie die Dateinamenverschlüsselung für die bereits bestehenden Dateien aktivieren.

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 entschlüsselten Dateien mit Ihrem Cloud-Anbieter synchronisiert werden, nutzen Sie bitte [Boxcryptor für macOS](#), [Boxcryptor für Windows](#) oder [Boxcryptor Portable](#).
- Falls Sie Ihre Dateien an einen anderen Ort oder in ein anderes Programm kopieren oder verschieben möchten, ist dies mit der Export-Funktion der Dateien-App möglich.

Kamera-Upload

Der Kamera-Upload sichert jedes Foto oder Video, das Sie mit Ihrem iPhone oder iPad gemacht haben. Alle neuen Fotos oder Videos werden **automatisch und verschlüsselt** unter **Boxcryptor Photos** bei Ihrem zuvor definierten Cloud Anbieter gespeichert.



Der Ordner und alle enthaltenen Dateien sind standardmäßig mit Dateinamenverschlüsselung versehen. Die Verschlüsselung des Dateinamens kann bei Kamera-Upload nicht deaktiviert werden und der Ordnername kann aus technischen Gründen nicht geändert werden.



Nicht alle Cloud-Anbieter unterstützen den Kamera-Upload, da nicht immer die erforderlichen Schreibrechte zur Verfügung stehen.

Um den Kamera-Upload zu aktivieren, führen Sie diese Schritte aus:

1. Öffnen Sie die **Boxcryptor-App** und navigieren Sie zu **Einstellungen**.
2. Tippen Sie auf **Kamera-Upload aktivieren**.
3. Erlauben Sie Boxcryptor, Benachrichtigungen zu senden sowie auf **alle** Ihre Fotos zuzugreifen.
4. Wählen Sie einen Cloud-Anbieter aus, auf den Sie die Dateien hochladen möchten. Wenn Sie nur einen kompatiblen Cloud-Anbieter zu Boxcryptor hinzugefügt haben, wird dieser

automatisch angezeigt und ausgewählt.

5. Wählen Sie aus, ob sie für den Upload auch **Mobile Daten verwenden** wollen.

Um den Kamera-Upload zu deaktivieren, tippen Sie erneut auf **Kamera-Upload aktivieren**.

Der Kamera-Upload ist als tägliche Aufgabe geplant und wird ausgeführt wenn folgende Bedingungen erfüllt sind:



- korrekte Netzwerkverbindung
- ladendes Gerät
- ausreichend verfügbare Rechenleistung

Das Auslösen des Kamera-Uploads liegt ausschließlich in der Verantwortung von iOS und kann durchaus 2-3 Tage dauern.



Wenn die Boxcryptor-App zwangsweise geschlossen wird (beispielsweise indem Sie zweimal auf den Home-Button tippen und die App wegswischen), **funktioniert der Kamera-Upload nicht mehr bis die Boxcryptor-App wieder geöffnet wird.**

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

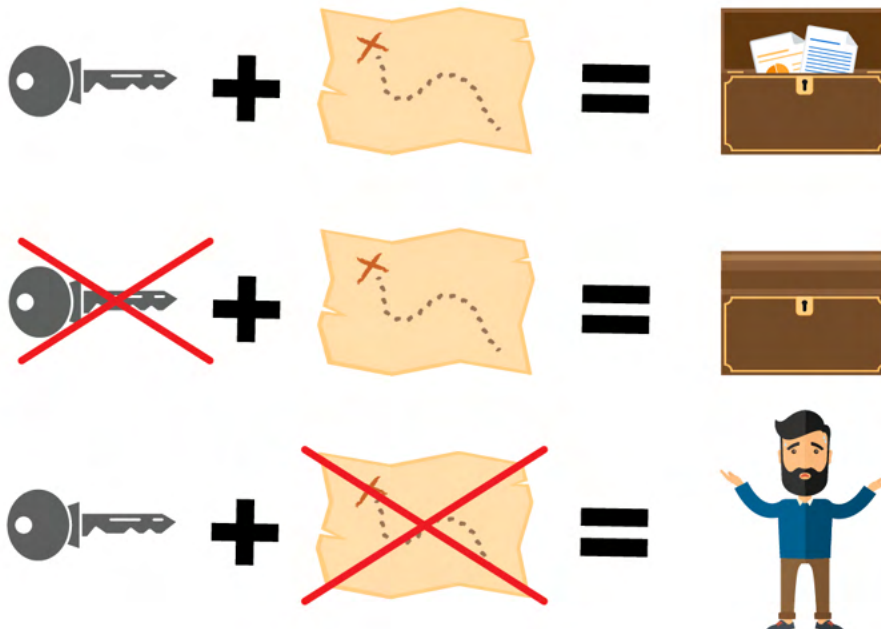
Um zu verstehen, wie das Teilen von verschlüsselten Dateien funktioniert, ist es hilfreich zu wissen, wie Programme unverschlüsselte und verschlüsselte Dateien behandeln.

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**.

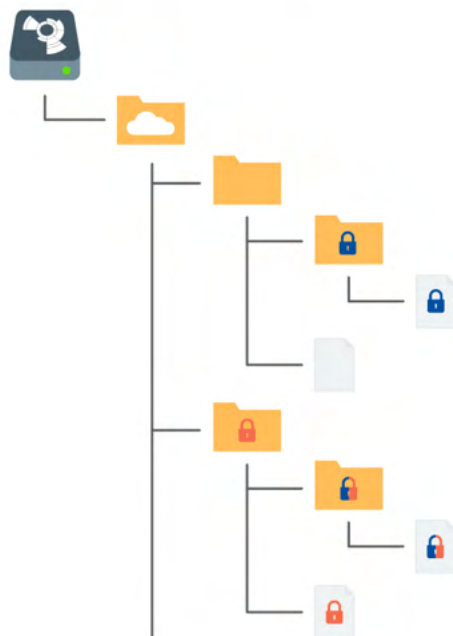
Deshalb sind zwei Schritte nötig, um eine verschlüsselte Datei zu teilen:

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

Verwalten von Berechtigungen ist mit Boxcryptor für iOS nicht möglich. Bitte verwenden Sie [Boxcryptor für Windows](#) oder [Boxcryptor für macOS](#), um Berechtigungen zu verwalten.

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. Whisply ist nicht in Boxcryptor für iOS integriert. Sie können [die Browser-Version von Whisply](#) verwenden, um Dateien oder Ordner mit Empfängern zu teilen, die nicht Boxcryptor nutzen.

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

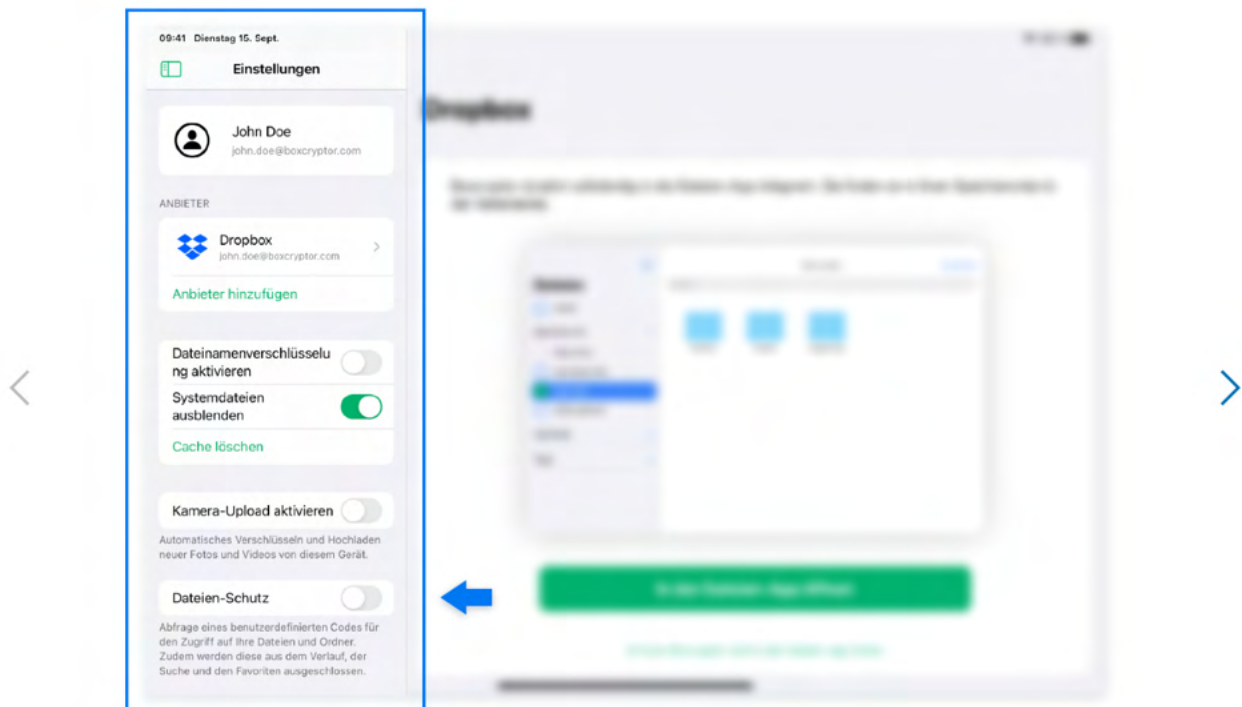
In Boxcryptor für iOS können Sie anstelle des App-Schutzes den **Dateien-Schutz** aktivieren. Der Dateien-Schutz verhindert unbefugten Zugriff auf **Dateien und Ordner im Boxcryptor-Speicherort in der Dateien-App**. Um die Funktion zu nutzen, müssen Sie in der Boxcryptor-App den entsprechenden Schalter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

Weitere Einstellungsmöglichkeiten:

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

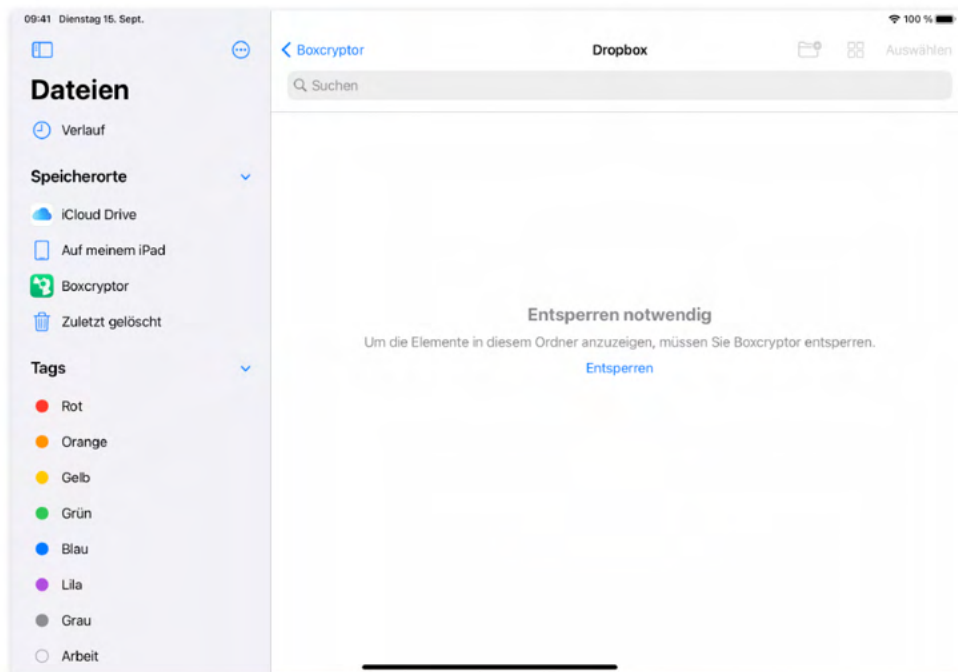


Für Änderungen an den Einstellungen des Dateien-Schutzes in der Boxcryptor-App ist immer eine erneute Eingabe des sechsstelligen Boxcryptor-Codes notwendig.



Dateien-Schutz aktivieren, Schritt 1: Schalter in der Boxcryptor-App aktivieren.

Wenn Sie nun den Boxcryptor-Speicherort in der Dateien-App öffnen, werden Sie aufgefordert, den Zugang mit dem neuen Boxcryptor-Code zu entsperren.



Boxcryptor Dateien-Schutz: Gesperrter Speicherort in der Dateien-App.



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

Technische Limitierungen

- Wenn Sie **In Dateien sichern** im gesperrten Zustand verwenden, wird der Boxcryptor-Speicherort deaktiviert angezeigt. Anschließend müssen Sie die Boxcryptor-App öffnen um den Dateien-Schutz zu entsperren.
- Die automatische, zeitbasierte Sperrung ist nicht mehr verfügbar, da wir Speicherorte nicht ohne Nutzer-Interaktion entfernen können. Um Ihre Dateien und Ordner lokal zu schützen müssen Sie den Dateien-Schutz manuell in der Boxcryptor-App sperren unter **Start -> Jetzt sperren**. Eine Benachrichtigung wird Sie daran erinnern, dass Ihre Dateien und Ordner ungeschützt sind.

Boxcryptor-Einstellungen

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

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

- [Speicherorte zu verwalten](#),
- [Dateinamenverschlüsselung](#) zu aktivieren,
- den [Kamera-Upload](#) einzurichten,

- **Systemdateien ausblenden**
- sowie das Boxcryptor-Konto **abzumelden** und die App auf Werkseinstellungen zurückzusetzen.

Files App Dokumentation

Weitere Informationen zur Funktionsweise und zur Arbeit mit der Dateien-App finden Sie in Apples eigener [Dokumentation](#).

◀ ZURÜCK

WEITER ▶

Boxcryptor-Konto

Ihr Konto verwalten

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

Passwort wiederherstellen

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



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

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

Geräte und Sitzungen verwalten

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

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

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

Schlüssel exportieren

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

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

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



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

Lokales Konto

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

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

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



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

✓ Eine Schlüsseldatei exportieren

Um ein lokales Konto zu verwenden, müssen Sie zunächst Ihre Schlüssel wie [hier](#) beschrieben exportieren.

Eine bestehende Schlüsseldatei öffnen

1. Schicken Sie die Schlüsseldatei an Ihr Gerät, zum Beispiel per E-Mail oder AirDrop.
2. Wählen Sie die Schlüsseldatei und senden diese an die Boxcryptor-App.
3. 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:

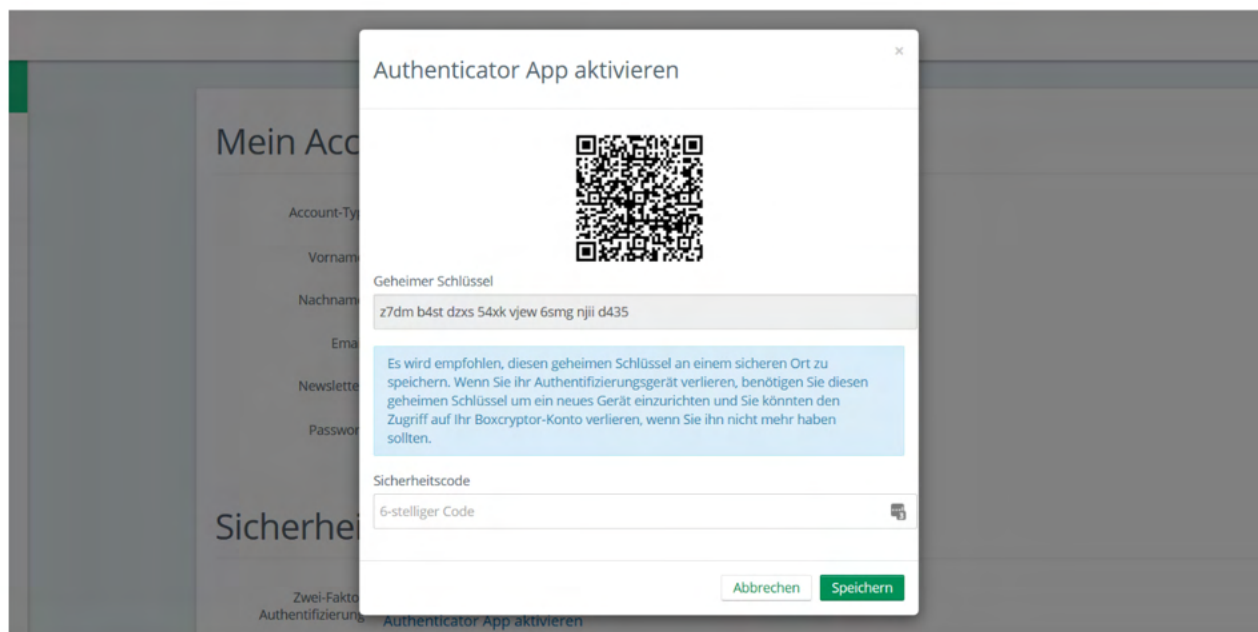
1. Melden Sie sich auf boxcryptor.com an.

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](#)



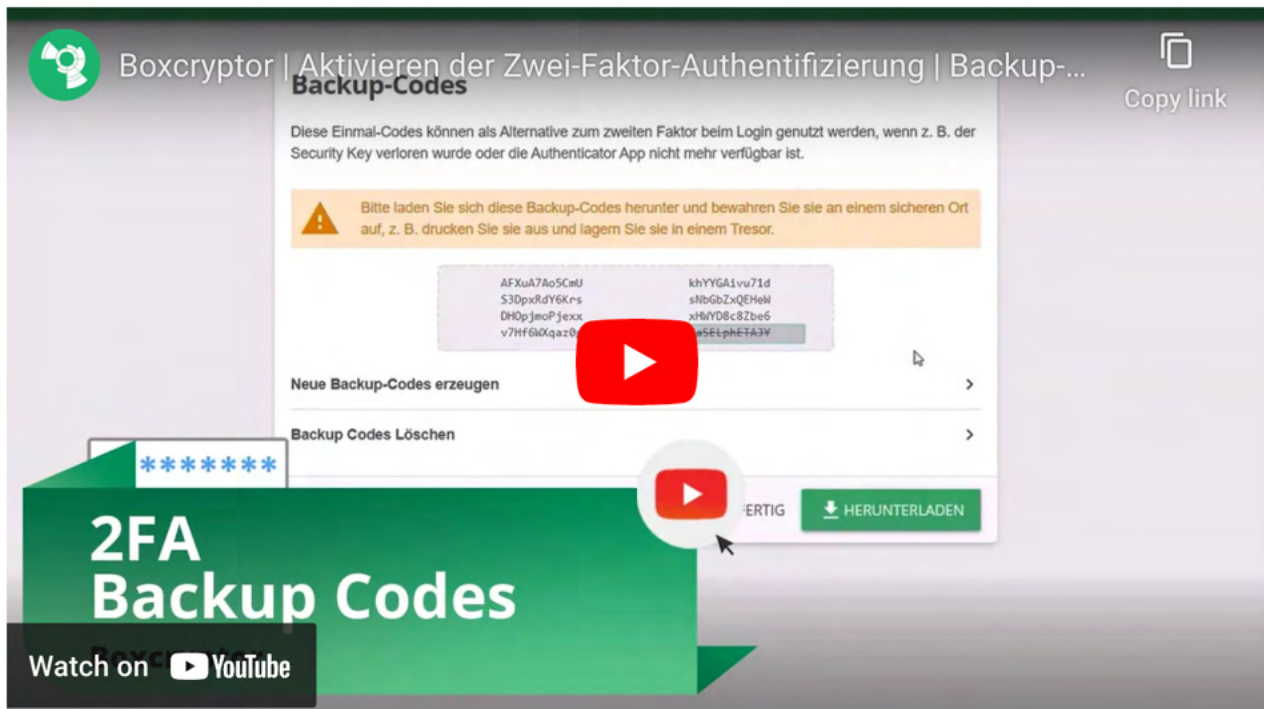
Um ein versehentliches Aussperren zu vermeiden empfehlen wir das Registrieren eines zweiten Security Keys. Nutzen Sie den Ersten für Ihre täglichen Geschäfte und bewahren Sie den Zweiten als Backup auf, falls Sie den ersten verlieren. Alternativ können Sie auch TOTP als zweiten Backup-Faktor einrichten.

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.

Um Ihre Dateien zu entschlüsseln, empfehlen wir die Verwendung von [Boxcryptor für macOS](#) oder [Boxcryptor für Windows](#).

Wenn Sie auf diesen Plattformen nicht auf Ihre Dateien zugreifen können, können Sie Ihre verschlüsselten Dateien und Ordner auch mit der Dateien-App auf Ihr iPhone oder iPad kopieren und einfügen.

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.](#)

Boxcryptor wird nicht in der Dateien-App angezeigt

In einigen Fällen wird Boxcryptor nach der Installation nicht direkt in der Dateien-App angezeigt.

Um dieses Problem zu lösen, muss das Gerät neu gestartet werden.

Selbstsignierte Zertifikate für Cloud Provider verwenden

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

Damit Boxcryptor eine Verbindung zu Ihrem Server herstellen kann, müssen Sie das selbstsignierte Zertifikat auf ihrem iPhone oder iPad installieren. Weitere Informationen zur Installation finden Sie [hier](#).

Weitere Informationen zu Apple's Zertifikatsanforderungen finden sie [hier](#).



Wenn Sie die Domäne besitzen, können Sie stattdessen ein **freies und vertrauenswürdigen Zertifikat** erstellen. Weitere Informationen finden Sie bei Zertifikatsausstellern wie [Let's Encrypt](#).

Ich kann keine Dateien in einen verschlüsselten Ordner verschieben

Das Verschieben von Dateien zwischen unterschiedlich verschlüsselten Ordnern oder in einen neuen verschlüsselten Ordner erfordert immer die erneute Verschlüsselung der Dateien mit einem neuen Schlüssel. Boxcryptor muss das Element herunterladen, entschlüsseln, verschlüsseln und das Element erneut hochladen. Dies würde eine offensichtliche Belastung für Ihre Datennutzung darstellen. Da der Nutzer nicht mit so viel benötigter Bandbreite für einen einfachen Verschiebe- / Kopiervorgang rechnet, haben wir beschlossen, die Option zum Verschieben und Kopieren zwischen verschlüsselten Ordnern zu deaktivieren.

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. Boxcryptor Classic für iOS ist nicht mehr im App Store verfügbar.

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*.

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

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

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

Enthält die Datei sensible Informationen?

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

Was passiert bei Verlust der Datei?

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

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

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

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

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

Enthält die Datei sensible Informationen? Kann ich sie löschen?

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

Account Zugriff bei verlorenem zweiten Faktor (2FA) wiederherstellen

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

Möglichkeiten, den Zugriff auf Ihr Konto wiederherzustellen:

✓ Den geheimen Schlüssel aus der Ersteinrichtung erneut anwenden

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

Als Referenz sieht der geheime Schlüssel ähnlich aus wie:

| mzwe wocd mj3d qr3f njjw g2cm grqw cvli

✓ Einen Gerätecode verwenden

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

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



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

✓ Einen Backup-Code einsetzen

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



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

✓ Keine der oben genannten Methoden sind möglich

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

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

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

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

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

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

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

iPhone und iPad: <https://apps.apple.com/app/microsoft-teams/id1113153706> Android:

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

Ungültige Codes der Authenticator App

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

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

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

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

Why Is Boxcryptor “Files App First”?

With iOS 11, Apple introduced the Files app as the central hub and designated way to work with files on iPhones and iPads in 2021. Besides the default storage locations iCloud and "On my device", apps like Boxcryptor can integrate with the Files app and provide their own files and folders. At the same time, other apps can integrate the Files app in order to seamlessly work with exactly those files.

The Files app is a huge improvement for workflows spanning multiple apps to get your work done. Our mission and promise at Boxcryptor is and has always been to secure your files stored in the cloud.

Our mission is to become the service of choice for everyone who wants to secure files in the cloud. Today, cloud computing is part of our everyday lives and it is continuously changing and evolving. The influence that cloud computing has on our personal and business lives will have a lasting impact on our world. Therefore, data security in the cloud is of highest priority. Personal and sensitive information are valuable property that must be protected – today and always. Boxcryptor was born inspired by our passion for cloud computing security and our wish to find new solutions to make our lives a little easier and more secure. As we grow, we will continue to protect information across devices in the cloud and to develop services and solutions as needs and wants evolve.

This [mission](#) is our guideline when developing Boxcryptor now and in the future. *Files app first* is an important step on this journey and ensures that we continue to meet our customer's requirements in 2021 and beyond. You can learn more about the advantages of the Files app [here](#).

Why Did You Remove Your Own File Browser?

On one hand, developing and maintaining your own files browser including all bells and whistles requires a huge effort, on the other hand it can never match the experience Apple is able to provide with the Files app due to its central and deep integration in iOS and other apps.

Focusing on the Files app integration allows us to provide a more clear user experience by having a single place to work with your encrypted files and also to optimize our development resources around our core value proposition: The best end-to-end encryption solution for cloud storages.

I Don't Trust Apple, iOS or the Files App

Apple owns the hardware, the operating system, and all core apps running on your iPhone or iPad. It is impossible to develop a third party iPhone or iPad app which can protect data against Apple as an attack vector.

If you do not trust Apple, iOS or the Files app, the only real solution is not to use an Apple device. You should only use devices and operating systems which have your trust.

App security always relies on operating system security and operating system security always relies on hardware security. Thus, trust is inherited: Hardware must be trusted to trust the operating system. The operating system must be trusted to trust an app. If trust for the hardware or operating system are missing, this trust can never be restored by an app.

The new Boxcryptor app is as secure as the old one was. Even if you disabled the Files app integration in the old app, Boxcryptor – just like every app - always used functionality provided by iOS, e.g. to perform the actual encryption and decryption or to preview files within the Boxcryptor app. Files in the Boxcryptor app have always been exposed to Apple's software and hardware - regardless if the Files app integration was used or not.

Just like iOS, the Files app adheres to the highest standards for privacy and data security found in the industry. Other apps can only access files in the Files app if you explicitly opened a file. **It is not possible that other apps secretly access your encrypted files in Boxcryptor via the Files app behind your back.** You can learn more about the security of Apple platforms [here](#).

I Don't Trust Other Apps

By default, the Files app automatically opens a file in another app if it supports the file type. For example, Word documents will automatically open in the Word or Office app if it is installed.

If you have apps installed which you don't trust, the only real solution is to uninstall them. You should only install and use apps which have your trust.

If you do not want that a specific file opens in another app, you can use the Quick Look feature of the Files app to preview a file directly in the Files app. You can learn more about it [here](#).

Sonstiges

Wartungsfenster

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

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

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

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

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

Changelog

Version 3.24 (2022-11-17)

- Fixed bug when adding cloud storage provider
- Fixed bug when unlock the Files Protection

Version 3.23 (2022-11-11)

- Fixed rename of a file name encrypted folder leads to access denied error
- Fixed files remain in waiting state while downloading or uploading
- Besides recent sites SharePoint now lists all sites the user has access to instead of only followed sites
- Minor bugfixes and improvements

Version 3.22 (2022-10-19)

- Fixed editing of Office files
- Improved SharePoint site and MS Teams Channel listing
- Improved local file cache cleanup
- Minor bugfixes and improvements

Version 3.21 (2022-09-28)

- Fixed large file uploads and downloads on iCloud
- Minor bugfixes and improvements

Version 3.20 (2022-08-30)

- Minor bugfixes and improvements

Version 3.19 (2022-08-01)

- Files Protection now removes Boxcryptor locations in Files App
- Improved Files Protection Manual Lock process
- Improved disk space consumption
- Fixed Clear Cache Button did not work properly
- Fixed bug when opening files on Strato HiDrive
- Removed Files Protection Auto-Lock
- Added device code to recover Account Access if Second Factor (2FA) is Lost
- Minor bugfixes and improvements

Version 3.18 (2022-06-08)

- Added LeitzCloud to our supported cloud storage provider list
- Minor bugfixes and improvements

Version 3.17 (2022-04-04)

- Fixed Google Drive deleted Shortcuts handling
- Fixed Share to Boxcryptor with enabled Files Protection
- Minor bugfixes and improvements

Version 3.16 (2022-03-21)

- Support Google Drive Shortcuts
- Fixed MagentaCLOUD authentication issues
- Fixed MagentaCLOUD connection issues
- Fixed usage of multiple Nextclouds at the same time
- Improved OneDrive error handling
- Minor bugfixes and improvements

Version 3.15 (2022-02-07)

- Added: Tabs for improved usability
- Improved: Each provider now has its own Boxcryptor location in the Files app
- Fixed: Old shared files cannot be decrypted

Version 3.14 (2021-12-04)

- Support new MagentaCLOUD

Version 3.13 (2021-12-02)

- Support new MagentaCLOUD

Version 3.12 (2021-10-05)

- Fixed: Boxcryptor sign-in after device change

Version 3.11 (2021-09-27)

- Fixed: Camera Upload may not start uploading

Version 3.10 (2021-09-20)

- iOS 15 Support
- Added Files Protection

Version 3.09 (2021-08-18)

- Minor bugfixes and improvements

Version 3.08 (2021-05-27)

- Minor bugfixes and improvements

Version 3.07 (2021-05-13)

- Minor bugfixes and improvements

Version 3.06 (2021-05-09)

- Minor bugfixes and improvements

Version 3.05 (2021-05-06)

- Minor bugfixes and improvements

Version 3.04 (2021-05-03)

- Minor bugfixes and improvements

Version 3.03 (2021-04-28)

- Files App First Find all your encrypted files in the Files App and only there.
- Security Keys Sign in with your security key for additional account protection.
- Microsoft Teams Work with encrypted files stored in Microsoft Teams.
- App Protection Removed Access to files in the Files app cannot be additionally protected.

Version 2.51.901 (2021-01-11)

- Minor bugfixes and improvements

Version 2.50.889 (2020-10-29)

- Minor bugfixes and improvements

Version 2.49.887 (2020-09-25)

- Minor bugfixes and improvements

Version 2.48.869 (2020-09-16)

- Official iOS 14 Support
- You can now add up to 5 photos at once
- Improved iCloud performance
- Improved Dropbox listing
- Minor bugfixes and improvements

Version 2.47.865 (2020-05-08)

- Minor bugfixes and improvements

Version 2.46.861 (2020-04-14)

- Added LeitzCloud to our supported cloud storage provider list
- Fixed Camera Upload uploading already uploaded photos.
- Minor bugfixes and improvements

Version 2.45.857 (2020-02-04)

- Minor bugfixes and improvements

Version 2.44.853 (2019-12-11)

- Minor bugfixes and improvements

Version 2.43.851 (2019-11-18)

- Minor bugfixes and improvements

Version 2.42.847 (2019-09-27)

- Minor bugfixes and improvements

Version 2.41.846 (2019-09-19)

- Official iOS 13 Support
- Beautiful new user interface
- Dark Mode support
- Minor bugfixes and improvements

Version 2.40.840 (2019-08-26)

- Fixed: Provider Box sometimes asks user for Credentials
- Improved: Connection to Provider HubiC
- Improved: Connection via WebDAV
- Removed: Outdated Cloud-Provider GrauData
- Minor bugfixes and improvements

Version 2.39.836 (2019-07-22)

- Minor bugfixes and improvements

Version 2.38.832 (2019-06-09)

- Benvenuto, bienvenida & bienvenue - Added Italian, Spanish and French localization
- Added: Provider Wasabi
- Added: Select any document library within a SharePoint site
- Improved: Connection to AmazonS3
- Improved: Connection to Mail.ru
- Improved: Connection to SugarSync
- Improved: Connection to Egnyte
- Improved: iOS PasswordManager support - Passwords can now be autofilled
- Fixed: Some files in iCloud can not be opened
- Fixed: Some files can not be added to Boxcryptor
- Fixed: Externally updated files sometimes not updated
- Minor bugfixes and improvements

Version 2.37.826 (2019-01-16)

- Minor bugfixes and improvements

Version 2.36.824 (2018-12-14)

- Improved: Reduced memory consumption
- Improved: Connection to Amazon Cloud Drive
- Improved: Connection to Yandex Disk
- Improved: Connection to iCloud
- Improved: Connection to Orange Cloud
- Fixed: Box sometimes displayed wrong dates
- Fixed: Files did not update on Favorites tab
- Minor bugfixes and improvements

Version 2.35.820 (2018-11-12)

- Improved: App start time
- Fixed: Sign in without internet connection does not work
- Added: Strato HiDrive special character filename support

Version 2.34.818 (2018-10-19)

- Improved: Files App integration
- Improved: Connection to Provider Box
- Improved: Connection to Provider MagentaCloud
- Improved: Connection to Provider HiDrive
- Minor bugfixes and improvements

Version 2.33.815 (2018-10-16)

- Minor bugfixes and improvements

Version 2.32.807 (2018-09-26)

- Minor bugfixes and improvements

Version 2.31.804 (2018-09-24)

- Improved: Connection to Provider GoogleDrive
- Improved: Connection to Provider OneDrive
- Fixed: OneDrive login not possible on small devices
- Minor bugfixes and improvements

Version 2.30.799 (2018-07-23)

- Improved: Files App Integration
- Fixed: Discovered directory handled as being unencrypted
- Fixed: Activities tab not cleaned at sign out
- Minor bugfixes and improvements

Version 2.29.797 (2018-07-16)

- Improved: Dropbox connection
- Fixed: FaceID fails on second attempt
- Fixed: WebDav login sometimes fails
- Minor bugfixes and improvements

Version 2.28.791 (2018-05-24)

- Updated: Privacy Policy

Version 2.27.790 (2018-05-17)

- Added: Russian localization
- Fix: App might signout user when adding a provider
- Minor bugfixes and improvements

Version 2.26.783 (2018-03-26)

- New: ownCloud and Nextcloud support
- Improved: 'Save to Boxcryptor' compatibility
- Added: Dropbox Team Spaces

Version 2.25.780 (2018-02-12)

- Extended WebDAV support
- Added Google Drive 'Shared with me' Directory
- Improved OneDrive Germany support
- Enhanced Spark Mail support
- Added Provider SharePoint 2013
- Minor bug fixes and improvements

Version 2.24.774 (2017-12-20)

- Minor bug fixes and improvements

Version 2.23.771 (2017-12-7)

- New Feature: German translation
- New Feature: Sharepoint site entry form
- Fixed: WebDAV Encoding
- Fixed: OneDrive Shared Directories did not update
- Fixed: Directories with dots were displayed as packages in Files app
- Minor bug fixes and improvements

Version 2.22.769 (2017-11-20)

- Fixes white screen after tour
- Improves Camera Upload stability

Version 2.21.764 (2017-11-13)

- Fixes to Camera upload
- Files App stability
- iCloud performance improvements
- "Shared With Me" Directory for OneDrive
- Hubic showed empty directories
- Small bug fixes

Version 2.20.756 (2017-09-29)

- Fixed: Downloading/Uploading failed in background configuration
- Fixed: Saving to Photos did not ask for permission
- Fixed: Create Directory did not work

Version 2.19.752 (2017-09-22)

- Fixed: Crashes for some devices
- Fixed: "Save to Boxcryptor" dialog did not display

Version 2.18.743 (2017-09-19)

- Files App Integration
- Fixed: WebDAV with HTTP
- Fixed: Camera Upload for videos

Version 2.17.726 (2017-09-12)

- Fixed: Blank screen on iOS 11 Beta
- Fixed: Camera Upload sometimes crashed
- Small bug fixes

Version 2.16.725 (2017-09-04)

- New Feature: Camera Upload: Automatically upload your photos and videos
- Fixed: Word zero KB files
- Fixed: Livedrive filename encryption
- Fixed: Working with Favorites tab

- Fixed: WebDAV multi-user issues
- Fixed: OneDrive shows wrong modified/created date

Version 2.15.722 (2017-08-15)

- Fixed: Crash for local accounts when policies were set.
- Fixed: Upload issue for Dropbox

Version 2.14.721 (2017-08-09)

- Improved: Faster access to large directories in OneDrive
- Fixed: Bug on OneDrive for large document uploads
- Various other bug fixes and improvements

Version 2.13.717 (2017-07-20)

- New: Create folder while choosing a place for an upload
- New: Google Drive Team Drives support
- Various other bug fixes and improvements

Version 2.12.715 (2017-07-10)

- Small Bugfixes

Version 2.11.711 (2017-06-26)

- New: Authentication window redesign
- New OneDrive Sign Up
- Small Bug fixes

Version 2.10.708 (2017-06-21)

- Improved: Extension access time and fault tolerance
- New: Allows working with files while offline
- Fixed: Issue of background upload finish
- Minor bug fixes and improvements to extension

Version 2.8.696 (2017-05-15)

- Minor bug fixes and improvements to local account

Version 2.7.693 (2017-05-02)

- Minor bug fixes and improvements

Version 2.7.690 (2017-03-27)

- New Provider: Orange
- New Provider: Mail.ru Hotbox
- Bugfix for Amazon S3

Version 2.7.686 (2017-03-15)

- New Feature: Highlight your favourite files
- New Feature: "Save to Boxcryptor" – App extension which allows uploading multiple files from other apps.
- New Feature: "Display Password"-option during sign in
- New Provider: HubiC
- New Provider: Magenta

Version 2.7.684 (2017-01-19)

- Fixed bug with local account

Version 2.7.681 (2016-12-21)

- New Icons and UI Improvements
- Photos taken with Boxcryptor are compressed to 80% quality.

Version 2.7.679 (2016-12-12)

- Improved: A share menu is displayed in case a file can't be previewed
- Small bug fixes for iOS 9 and Document Extension
- Various stability improvements

Version 2.7.678 (2016-12-07)

- Major performance and stability improvements
- New: Search in folders
- New: Support for SharePoint Online
- New: Take photos directly within the Boxcryptor app
- Improved: Display of recent activities
- Improved: Open and edit files in third party apps
- Improved: Yandex support (Please re-add your account)
- Various other bug fixes and improvements

Version 2.6.444 (2016-10-20)

- N/A

Version 2.5.439 (2016-09-28)

- N/A

Version 2.5.435 (2016-09-26)

- N/A

Version 2.5.434 (2016-09-12)

- N/A

Version 2.5.433 (2016-05-27)

- N/A

Version 2.5.431 (2016-05-17)

- N/A

Version 2.5.430 (2016-05-10)

- N/A

Version 2.4.401 (2015-04-07)

- N/A

Version 2.3.401 (2014-04-09)

- N/A

Version 2.2.405 (2014-03-11)

- N/A

Version 2.2.403 (2014-02-20)

- 64bit support on newer iPhones & iPads
- Fixed: Box connection settings

Version 2.2.402 (2013-12-05)

- Fixed: crash on start-up when connected to SkyDrive

Version 2.2.401 (2013-12-01)

- Fixed: crash on start-up after update, when connected to SkyDrive
- Fixed: crash when trying to use a newly imported KeyFile

Version 2.2.400 (2013-11-25)

- Local Accounts
- Create new accounts
- iOS 7 UI
- Support for Cloudme & GRAU DATA providers
- Fixes for SkyDrive, LiveDrive
- Various fixes and improvements

Version 2.1.1 (2013-09-02)

- Fixed: "Infinite Unlocking" issue
- Fixed: uploads from FileDrop
- Fixed: wrong handling of decrypted files which can't be viewed in the builtin previewer
- Other minor fixes and improvements

Version 2.1 (2013-08-14)

- (Beta) Encrypt & upload files (including photos and videos from the Photo Library)
- FileDrop, a local folder where you can store files (encrypted and plain) that are opened from other applications.
- Improved log in handling and session restore
- Option to enable/disable automatic log in
- Option to enable/disable filename encryption
- Improved "Add new Provider"
- File browser shows all files: Non-encrypted files have a black font color and encrypted files have a green font color.
- Improved "User Account Info"
- Fixed: Crash on log in with new accounts
- Fixed: Various WebDAV issues
- Fixed: SugarSync & Yandex Disk log in issues

Version 2.0.1 (2013-06-11)

- Improved: Performance

Version 2.0 (2013-05-31)

- 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](#)