Einführung

Was ist die Cloud?

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

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

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

Was ist Boxcryptor?

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

Was Boxcryptor **nicht** ist

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

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

Quickstart

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

Boxcryptor installieren

Systemvorraussetzungen: Benötigt mindestens Android 6.0. Boxcryptor für Android ist mit Smartphones und Tablets kompatibel.

Um Boxcryptor zu installieren, laden Sie die Boxcryptor-App aus dem Google Play Store herunter.

> Auf Android-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.

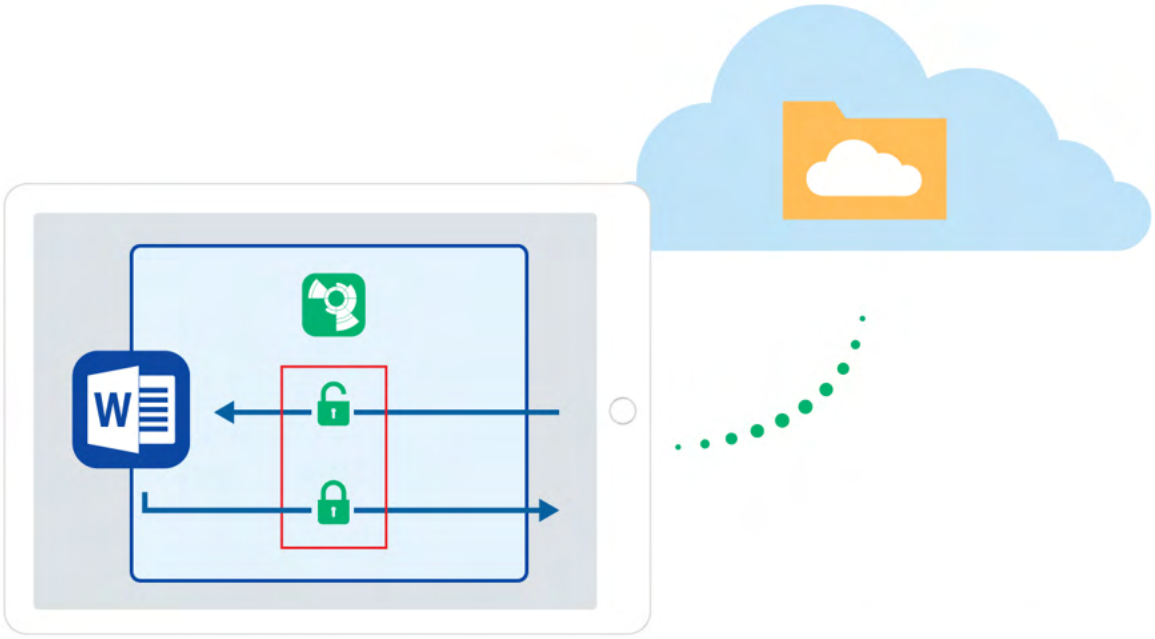
> Wenn Sie Ihr Passwort vergessen, sind Ihre Daten irreversibel verloren.

Entdecken Sie Boxcryptor

Nachdem Sie Boxcryptor installiert und sich mit Ihrem Boxcryptor-Konto angemeldet haben, können Sie Ihren Cloud-Anbieter hinzufügen und auf Ihre Dateien zugreifen.

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

Ihrer Dateien, sowie um die Entschlüsselung.



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

Sie können Boxcryptor direkt aus anderen Apps herau nutzen, beispielsweise in Word. Wenn Sie eine Word-Datei ändern wollen, öffnen Sie Word → wählen Sie **Öffnen anderer Dokumente** auf dem **Öffnen**-Register, → **Durchsuchen** → → wählen Sie **Boxcryptor**.

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 die **Boxcryptor-Anwendung**.
2. Öffnen Sie Ihren Cloud-Anbieter in der Boxcryptor-Anwendung.
3. Drücken Sie auf → **Neuer Ordner**.
4. Geben Sie einen Namen für den neuen Ordner an. Die Verschlüsselung ist vorausgewählt.
5. Laden Sie Dateien oder Fotos in den Ordner. Alle Dateien werden automatisch verschlüsselt.

Wie man bestehende Dateien verschlüsselt

Das Verschlüsseln von bereits existierenden Dateien ist mit Boxcryptor für Android derzeit 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 Android **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. Tippen Sie auf ☰.
2. Tippen Sie auf **Einstellungen** und **Speicherorte Verwalten**.
3. In Ihrer Anbieter Übersicht tippen Sie auf das **Plus Zeichen in der unteren rechten Ecke**.
4. **Wählen Sie nun Ihren Anbieter aus** und geben Sie die Zugangsinformationen Ihres Anbieters ein, um ihn mit Boxcryptor zu verbinden.

Google Drive

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

Benutzerdefinierte Speicherorte

Boxcryptor unterstützt das Hinzufügen von Ordnern auf Ihrer SD-Karte oder aus Ihrem internen Speicher als **lokaler Speicher**:

1. Tippen Sie auf ☰.
2. Tippen Sie auf **Einstellungen** und **Speicherorte Verwalten**.
3. In Ihrer Anbieter Übersicht tippen Sie auf das **Plus Zeichen in der unteren rechten Ecke**.
4. Tippen Sie auf **Lokaler Speicher** und wählen Sie Ihre Geräte und Ihren eigenen Speicherort.

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 unterstützt wird.

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

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

2. Tippen Sie auf ☰.

3. Tippen Sie auf **Einstellungen** und **Speicherorte Verwalten**.
4. In Ihrer Anbieter Übersicht tippen Sie auf das **Plus Zeichen in der unteren rechten Ecke**.
5. Tippen Sie auf **WebDAV Advanced** und geben Sie die WebDAV-Zugangsdaten Ihres bevorzugten Cloud-Anbieters ein.

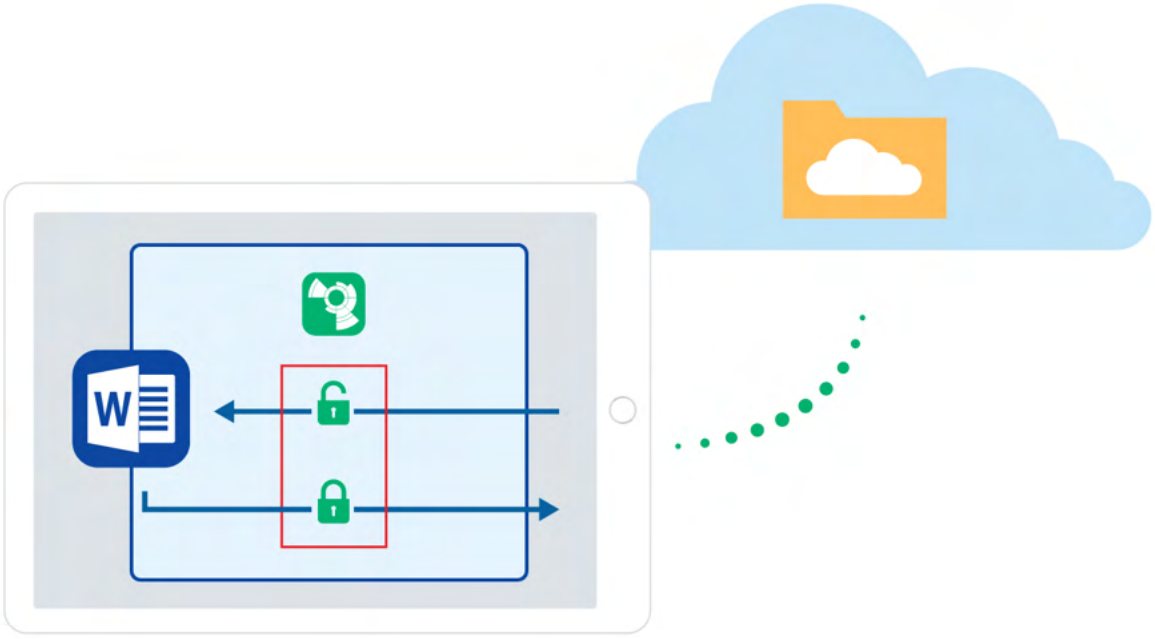
ownCloud und **nextCloud** unterstützen WebDAV. Standardmäßig lauten die Konfigurations-URLs:
`https://example.com/owncloud/remote.php/webdav`
`https://example.com/nextcloud/remote.php/dav/files/username/`

Mit Dateien arbeiten

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

On-the-Fly-Verschlüsselung

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



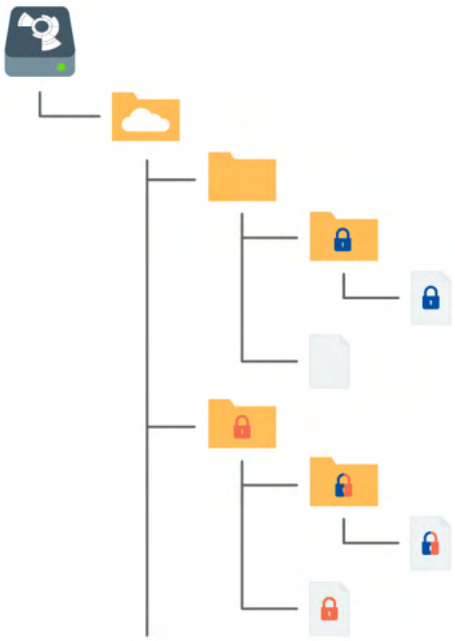
Wir entschlüsseln und verschlüsseln Ihre Dateien On-Demand: Sie wollen Ihre Inhalte sehen? Tippen Sie nur darauf und wir laden Ihre Datei für Sie herunter und entschlüsseln diese. Haben Sie Ihren Essay fertiggestellt? Senden Sie ihn einfach an Boxcryptor und wir verschlüsseln die Datei und speichern 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 fragen, ob Sie das Objekt verschlüsseln möchten oder nicht.

Mit Ihren Dateien arbeiten

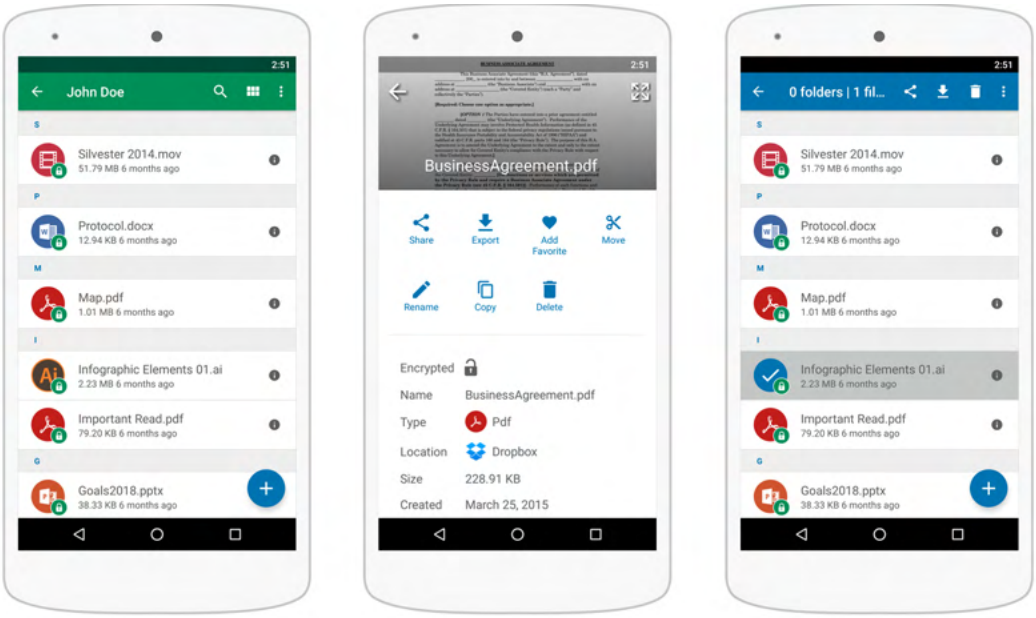
Mit Boxcryptor müssen Sie **Dateien nicht manuell entschlüsseln** um damit zu arbeiten. Die Boxcryptor-App ist ein Allzweck- **Datei-Browser**. Sie können in Ordner oder Vorschau-Dateien browsen, indem Sie darauftippen. Boxcryptor wird diese für Sie **automatisch herunterladen und entschlüsseln**. Sie können Dateien hochladen, neue Dateien und Ordner erstellen oder Sie können verschlüsselte Fotos aufnehmen, indem Sie auf + tippen.

Wenn Sie eine Datei lange gedrückt halten, wechselt der Dateimanager zum **Operation Modus**. In diesem Modus können sie Dateien und Ordner auswählen, indem Sie darauf tippen. Alle verfügbaren Operationen, wie zum Beispiel **kopieren, verschieben, umbenennen oder löschen** können im Balken oben ausgelöst werden.

Durch Tippen auf ⓘ gelangen Sie zur Detailansicht der Datei. In diesem Fenser sehen Sie eine **Vorschau der Datei und sie können diverse einfache Funktionen** vornehmen, wie kopieren, verschieben, umbenennen oder löschen.

Zusätzlich ermöglicht Boxcryptor, dass Sie eine Datei als **Favoriten** markieren- Alle als Favoriten markierten Dateien können einfach via ☰ → **Favoriten** geöffnet werden..

Die Ansicht Aktivitäten ☰ → **Aktivitäten**) zeigt alle kürzlich geänderten Dateien.



Dateien bearbeiten

Auf Android ist das Ändern von Dateien schwieriger als auf anderen Plattformen. Um die Sicherheit zu erhöhen, isoliert Android die einzelnen Apps. Das bedeutet, dass jede App nur auf die eigenen Ordner im System zugreifen kann. Dadurch können installiere Apps auf keine Daten anderer Apps zugreifen.

Das Problem: Falls Sie nun eine Datei mit einer anderen App, wie zum Beispiel Word teilen oder freigeben, wird die Datei an einen anderen Ort kopiert und Boxcryptor hat keinen Zugriff mehr darauf.

Aus diesem Grund integriert sich Boxcryptor in das Android Storage Access Framework, welches von anderen Apps benutzt werden kann. Falls Sie Dateien bearbeiten, stellen Sie sicher, dass Sie das immer mit der anderen App und nie mit Boxcryptor tun. Wenn sie beispielsweise eine Word-Datei ändern möchten, öffnen Sie Word → wählen Sie **anderes Dokument öffnen** auf dem **Öffnen**-Reiter, → **Durchsuchen** → ☰ → und wählen Sie **Boxcryptor**.

Wie Sie verschlüsselte Dateien erkennen

Boxcryptor ermöglicht es Ihnen, **verschlüsselte und unverschlüsselte** Dateien und Ordner im gleichen Verzeichnis zu verwalten. Verschlüsselte Dateien oder Ordner sind mit einem Symbol markiert. Bevor Sie neue Dateien oder Verzeichnisse erstellen, können Sie entscheiden, ob diese verschlüsselt werden sollen.

verschlüsselt

Verschlüsselung vorhandener Dateien und Ordner

Das Verschlüsseln bereits vorhandener Dateien ist derzeit nicht möglich mit Boxcryptor für Android. 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: 恟悰捋抱砻挼殥栟瞻擱斀漢怏搬濂檬溮楻捷抪柜欀睥.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.

Gehen Sie zu ☰ → **Einstellungen** → **Allgemein** und aktivieren Sie **Dateinamenverschlüsselung**.

> Bereits bestehene Dateien ohne Dateinamenverschlüsselung bleiben unverändert. Bitte benutzen Sie eines unserer Desktop-Programme, um die Dateinamenverschlüsselung auf bestehenden Dateien zu 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, benutzen Sie bitte Boxcryptor für Windows, Boxcryptor für macOS oder Boxcryptor Portable.
- Wenn Sie Ihre entschlüsselten Dateien an einen anderen Ort oder in eine andere App kopieren oder verschieben möchten, erlaubt Ihnen der Datei-Browser die unverschlüsselte Ansicht und die Möglichkeit die Dateien zu einer anderen App zu exportieren.

Kamera-Upload

Der Kamera-Upload sichert jedes Foto oder Video, das Sie mit Ihrem Smartphone oder Tablet 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.

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

1. Tippen Sie auf ☰ → Einstellungen
2. Tippen Sie auf **Automatischen Kamera-Upload Aktivieren**.
3. Wählen Sie die Cloud/den Speicherort aus, auf den Sie die Dateien hochladen möchten. Wenn Sie nur eine Cloud/einen Speicherort zu Boxcryptor hinzugefügt haben, wird diese/dieser automatisch angezeigt und ausgewählt.
4. Wählen Sie aus, ob Sie nur über eine Wlan-Verbindung oder auch über eine mobile Verbindung (Datentarif) hochladen möchten.
5. Um den Kamera-Upload zu deaktivieren, tippen Sie erneut auf **Automatischen Kamera-Upload Aktivieren**.

Mit Offline-Dateien arbeiten

Die Funktion **Offline-Dateien** ermöglicht es Ihnen jederzeit und ohne Internetverbindung auf Ihre verschlüsselten Dateien zuzugreifen.

Dazu können Sie eine gewünschte Datei auswählen und durch Klick auf ⋮ offline verfügbar machen.

Die Datei steht Ihnen anschließend unter **Offline-Dateien** verschlüsselt zur Verfügung.

Wenn die Datei in der Cloud aktualisiert wird, aktualisiert sich die Offline-Datei nach ca. 15 Minuten automatisch. Es ist allerdings auch möglich eine manuelle Synchronisation zu starten: Gehen Sie im Hauptmenü auf **Offline-Dateien**. Tippen Sie auf ⋮ und wählen Sie **Synchronisieren** aus.

Wenn Sie eine Änderung an einer Offline-Datei vornehmen, wird wie gewohnt ein automatischer Upload gestartet.

> Die **Offline-Dateien**-Funktion steht Ihnen ab **Version 2.85.736** zur Verfügung.

Zugriff auf Dateien teilen

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

Was Sie über das Teilen von verschlüsselten Dateien wissen müssen

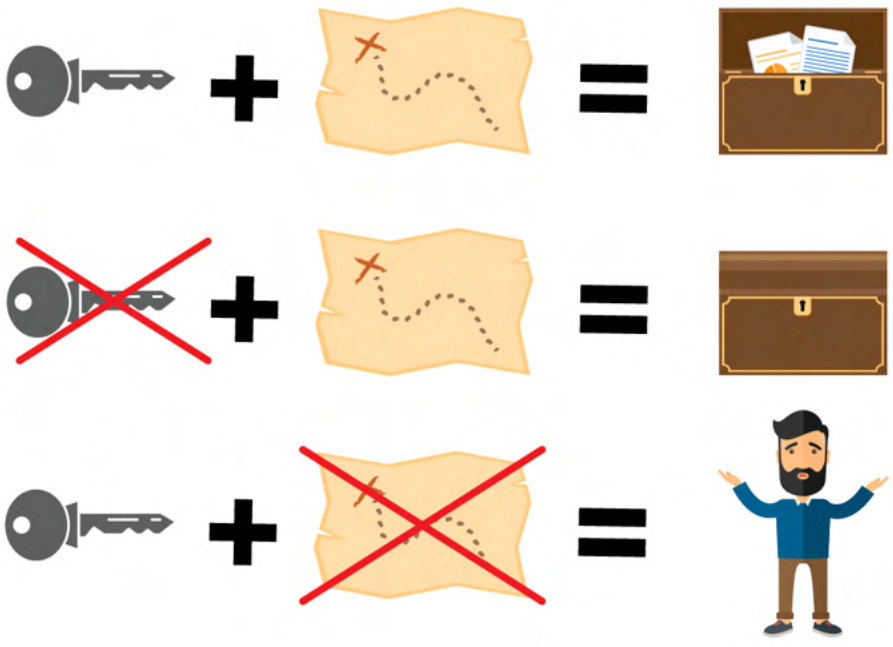
Um zu verstehen, wie das Teilen von verschlüsselten Datein funktioniert, ist es hilfreich zu wissen, wie Programme unverschlüsselte und verschlüsselte Datein behandeln.

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

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

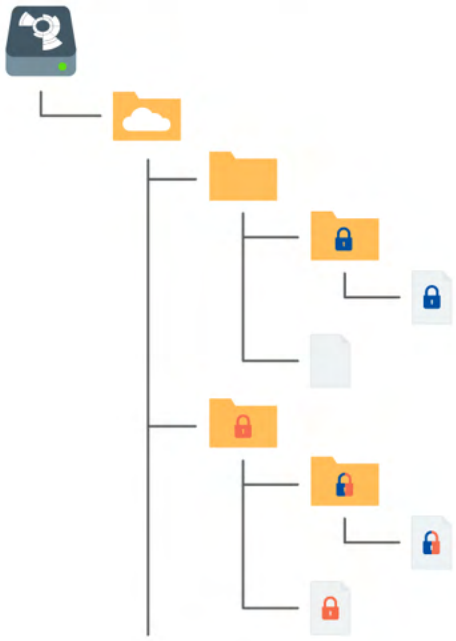
Deshalb sind zwei Schritte nötig, um eine verschlüsselte Datei zu teilen:

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



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

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



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

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

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

Dateien mit Boxcryptor-Nutzern teilen: Berechtigungen

Verwalten von Berechtigungen ist mit Boxcryptor für Android 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 Android 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 **Umbennnen**, **Löschen** oder **Eigentumsrechte gewähren** und **entziehen** kann nur der Besitzer der Gruppe (**Eigentümer**) vornehmen. Sie können andere Mitglieder als Eigentümer festlegen und ihnen die Eigentumsrechte auch entziehen. Gruppen können mehrere verschiedene Eigentümer haben.

Vorteile von Gruppen

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

Vorteile von Gruppen:

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

Einstellungen

App-Schutz

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

Wenn diese Funktion aktiviert ist, müssen Sie sich mit einer in Ihrem Gerät festgelegten Methode authentifizieren, um Boxcryptor verwenden zu können.

Um den App-Schutz verwenden zu können, muss mindestens eine der folgenden Schutzmethoden in den **Gerätesicherheitseinstellungen** aktiviert sein:

- **Muster**
- **PIN**
- **Passwort**
- **Fingerabdruck** (falls Hardware verfügbar)
- **Gesichtsentsperrung** (falls Hardware verfügbar)

Je nach Hardwarehersteller können die für Boxcryptor verfügbaren Schutzmethoden variieren. Für einige Geräte kann eine **primäre biometrische Authentifizierungsmethode** ausgewählt werden.

Der App-Schutz wird aktiviert, sobald sich die App im Hintergrund befindet oder das Gerät gesperrt ist. Wenn der Benutzer eine **biometrische** Authentifizierungsmethode verwendet, kann er Boxcryptor auch mithilfe einer alternativen Methode entsperren.

Der App-Schutz von Boxcryptor verwendet die neueste **AndroidX Biometric Library**. Bei manchen Geräten mit einem modifizierten Authentifizierungsbildschirm können Kompatibilitätsprobleme auftreten. Bei Problemen empfehlen wir, zunächst die Verwendung alternativer Schutzmethoden zu vermeiden und zu warten, bis der Gerätehersteller das Problem behoben hat.

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.
2. Wählen Sie die Schlüsseldatei und senden diese an die Boxcryptor-App. Haben Sie sich vorher noch nicht bei Boxcryptor angemeldet, werden Sie nun zu einer Anmeldeseite geleitet.
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.

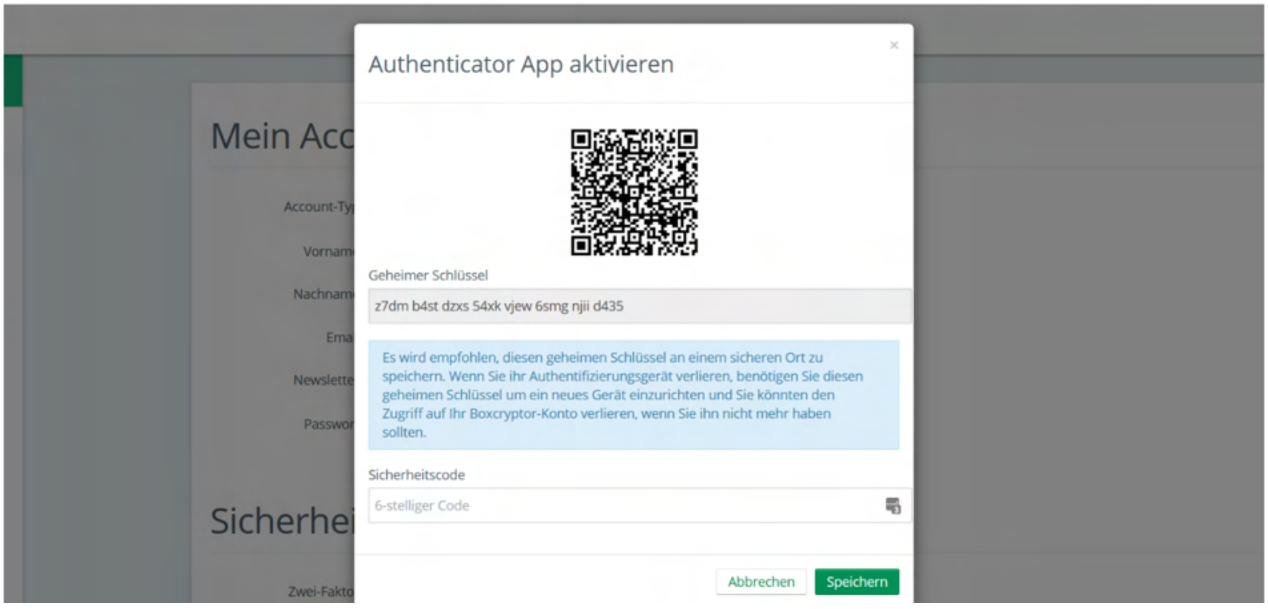
Authenticator-App

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.

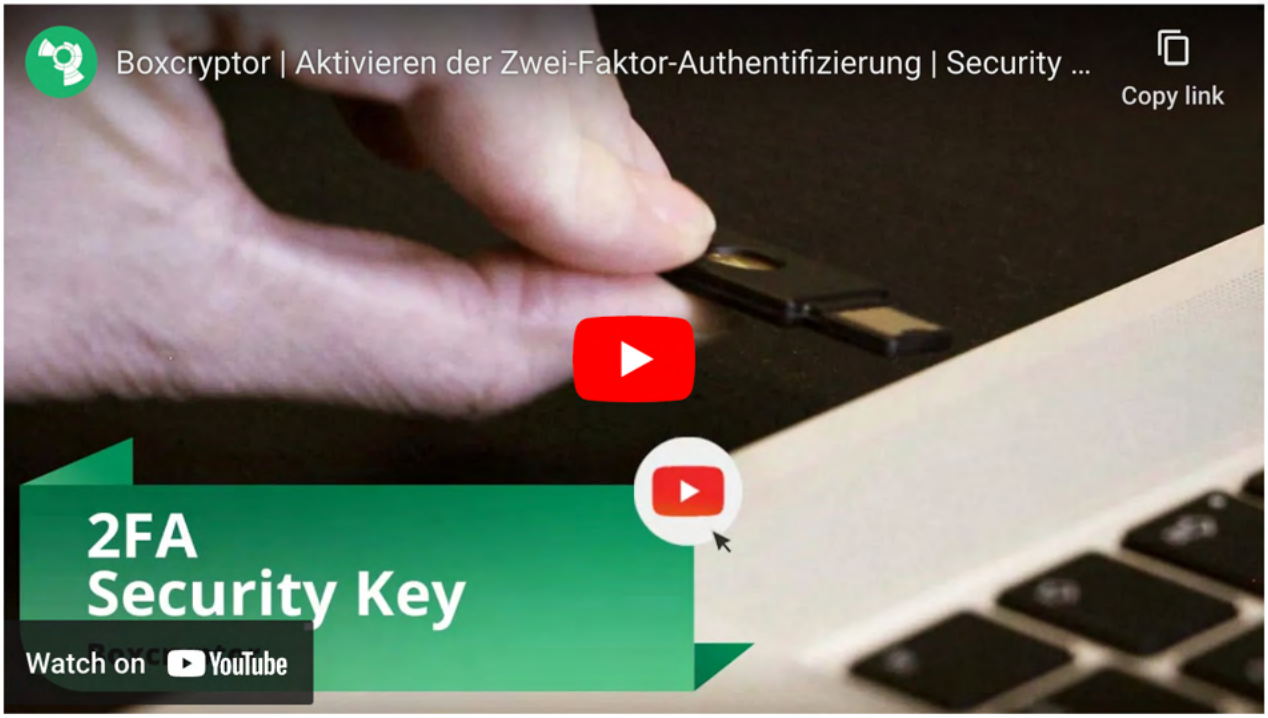
Security Keys

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



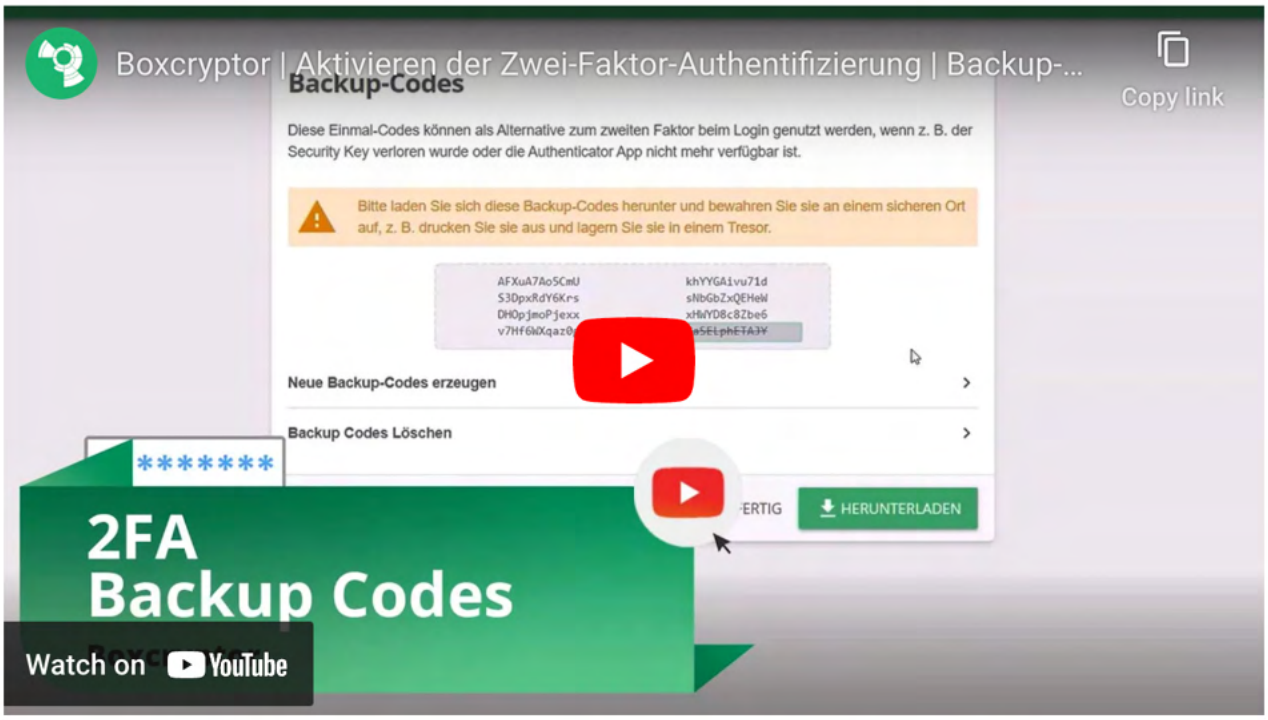
Um ein versehentliches Aussperren zu vermeiden empfehlen wir das Registrieren eines zweiten Security Keys. Nutzen Sie den Ersten für Ihre täglichen Geschäfte und bewaren Sie den Zweiten als Backup auf, falls Sie den ersten verlieren. Alternativ können Sie auch TOTP als zweiten Backup-Faktor einrichten.

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

Backup-Codes

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

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



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

2FA und die App-Schutz

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

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

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

FAQ & Fehlerbehebung

Off-Migration Guide: Alle mit Boxcryptor verschlüsselten Dateien entschlüsseln

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

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

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

Migration Tips für Unternehmen

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

Um Ihre Dateien zu entschlüsseln, empfehlen wir dringend die Verwendung von Boxcryptor für Windows oder Boxcryptor für macOS.

Wenn Sie auf diesen Plattformen nicht auf Ihre Dateien zugreifen können, verwenden Sie bitte die `Download`-Funktion, die für Dateien im Boxcryptor-Dateibrowser verfügbar ist.

Wenn Sie ganze Ordnerstrukturen exportieren müssen, empfehlen wir die Verwendung eines Drittanbieter-Tools, das über das „Storage Access Framework" auf Boxcryptor zugreifen kann: Dateien

Hier können Sie den Boxcryptor-Speicherort durchsuchen und jeden verschlüsselten Ordner über `lang drücken -> kopieren` und z.B. in Ihren Download`-Ordner 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.

Ich kann mich nicht mit den Boxcryptor-Servern verbinden

Proxy-Unterstützung

Boxcryptor nutzt die vom System bereitgestellt Proxy Konfiguration.

Hilfe hierzu finden Sie hier unter **Erweiterte Netzwerkeinstellungen → Proxy**.

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 als **Benutzerzertifikat** auf Ihrem Android-Gerät installieren. Weitere Informationen dazu finden Sie hier.

Für selbstsignierte Zertifikate ist bei der Erstellung der folgende Konfigurationseintrag erforderlich, um als gültige Stammzertifizierungsstelle akzeptiert zu werden: **`basicConstraints=CA:TRUE`**

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

Ich kann keine Dateien in einen verschlüsselten Ordner verschieben

Das Verschieben von Dateien zwischen unterschiedlich verschlüsselten Ordnern oder in einen neuen verschlüsselten Ordner erfordert immer die erneute Verschlüsselung der Dateien mit einem

neuen Schlüssel. Boxcryptor muss das Element herunterladen, entschlüsseln, verschlüsseln und das Element erneut hochladen. 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.

Der Kamera-Upload funktioniert nicht

Falls der Kamera-Upload nicht funktioniert, versuchen Sie Folgendes:

- **Beenden erzwingen**: Bitte erzwingen Sie nicht das Schließen von Boxcryptor mit einem App-Manager oder in den Android-Einstellungen, da dies auch jegliche Hintergrunderkennung beendet. **Starten Sie** Boxcryptor **neu**, um die Hintergrunderkennung erneut zu aktivieren.
- **Energie sparen**: Falls der Android-Batteriesparmodus aktiv ist, wird die Hintergrunderkennung blockiert. Sie können Boxcryptor im Vordergrund starten oder einfach den Batteriesparmodus deaktivieren.
- **Akku-Optimierung**: Android optimiert automatisch den Akkuverbrauch jeder installierten App. Dies kann Probleme verursachen, wenn ein Prozess im Hintergrund laufen muss, wie zum Beispiel Fotos und Videos erkennen. Sie können **Boxcryptor von der Optimierung ausschliessen**, indem Sie in den **Android Einstellungen unter Akku** → ⋮ → **Akku optimierungen** → **alle Apps** bis zu Boxcryptor scollen und „nicht optimieren" auswählen.
- **Boxcryptor neu starten**: In einigen Fällen reicht es, Boxcryptor neu zu starten. Schieben Sie Boxcryptor von den kürzlich verwendeten Android-Apps weg und starten Sie Boxcryptor erneut, damit die Erkennung für den Kamera-Upload neu gestartet wird.

Wo kann ich Boxcryptor Classic herunterladen?

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

Wenn Sie bereits Kunde von Boxcryptor Classic sind, können Sie es hier herunter laden. Außerdem sollten Sie so schnell wie möglich auf Boxcryptor upgraden. Boxcryptor Classic für Android ist nicht mehr in Google Play verfügbar, kann aber hier heruntergeladen werden: https://www.boxcryptor.com/download/Boxcryptor_Classic_v1.5.4_Android.apk *Unterstützt Android 2.1, 3, 4*

Veraltete Versionen

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

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

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

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

> neueste Version.

> Diese Client ID ist ungültig!

> Dies ist keine sichere Verbindung

> Das Remotezertifikat ist laut Validierungsverfahren ungültig

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

Lösung

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

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

Ich verwende Windows XP oder Mac OS X 10.14 oder früher

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

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

Ich kann nicht auf die neueste Version aktualisieren

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

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

Boxcryptor Portable

Boxcryptor Portable erfordert keine Installation und kann somit auch ohne Administratorenrechte verwendet werden um auf Ihr verschlüsselten Dateien zuzugreifen

und diese zu entschlüsseln. Sie können Boxcryptor Portable hier herunterladen.

Schlüsselexport

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

Ich kann mich wegen zu vieler verbundener Geräte nicht anmelden

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

Manche Dateien lassen sich nicht öffnen

Probleme beim Boxcryptor-Zugriff

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

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

Probleme mit den Dateisystem-Berechtigungen

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

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

Sync-Probleme

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

> Datei öffnen zeigt "Beim Dekodieren ungültige Daten gefunden" und

> die .bc-Datei ist leer.

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

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

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

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

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

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

Enthält die Datei sensible Informationen?

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

Was passiert bei Verlust der Datei?

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

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

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

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

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

Enthält die Datei sensible Informationen? Kann ich sie löschen?

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

Account Zugriff bei verlorenem zweiten Faktor (2FA) wiederherstellen

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

Möglichkeiten, den Zugriff auf Ihr Konto wiederherzustellen:

Den geheimen Schlüssel aus der Ersteinrichtung erneut anwenden

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

Als Referenz sieht der geheime Schlüssel ähnlich aus wie:

> mzwe wocd mj3d qr3f njjw g2cm grqw cvli

Einen Gerätecode verwenden

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

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

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

Einen Backup-Code einsetzen

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

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

Keine der oben genannten Methoden sind möglich

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

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

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

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

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

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

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

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

Ungültige Codes der Authenticator App

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

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

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

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

Sonstiges

Wartungsfenster

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

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

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

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

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

Changelog

Gaps in the changelog represent internal test versions.

Version 2.122.1101 (2022-10-18)

- Fixed download issues on Dropbox
- Minor bugfixes and improvements

Version 2.121.1099 (2022-09-20)

- Fixed startup issues on Android 6

Version 2.120.1098 (2022-09-15)

- Fixed issues due to which uploads were not allowed to start
- Fixed issues where details for failed uploads were not available
- Fixed issues with video preview
- Reduced memory consumption
- Minor bugfixes and improvements

Version 2.119.1095 (2022-09-01)

This version has **official support for Android 13**.

- Official Android 13 support
- Fixed issues when sharing files with other apps
- Improved performance
- Minor bugfixes and improvements

Version 2.116.1072 (2022-08-03)

- Fixed issues with automatic camera upload
- Minor bugfixes and improvements

Version 2.115.1066 (2022-06-09)

- We added zoom functionality for the in-App Camera
- Favourites and offline files are now also displayed in the Storage Access Framework
- Fixed issues where files couldn't get uploaded to IONOS
- Minor bugfixes and improvements

Version 2.114.1057 (2022-04-06)

- Fixed issues while working without internet connection
- Fixed issues where uploads or downloads could get stuck in waiting state
- Fixed issues with special Google Drive file types
- Minor bugfixes and improvements

Version 2.113.1054 (2022-02-03)

- Fixed issues with uploading multiple files
- Fixed issues when working in external applications
- Fixed issues with Google Drive shortcuts
- Fixed issues where the specified network type was ignored for downloading files available offline
- Fixed issues with previewing audio and video files
- Minor bugfixes and improvements

Version 2.112.1047 (2021-12-06)

- Minor bug fixes and improvements

Version 2.111.1042 (2021-12-01)

- Support new MagentaCLOUD

Version 2.110.1036 (2021-10-19)

- Minor bug fixes and improvements

Version 2.109.1034 (2021-10-04)

This version has **official support for Android 12**.

This version **does not support Android Lollipop (5)** anymore. As this old version is not supported by Google anymore, we recommend affected users to **update the operating system** to a newer version as soon as possible in order to stay safe.

- Official Android 12 support
- Minor bug fixes and improvements

Version 2.108.1021 (2021-08-04)

- We added Microsoft Teams to our supported cloud storage provider list
- We added dark mode support
- Changed colour scheme of the user interface
- Fixed caching issues

Version 2.107.1005 (2021-06-23)

- When using the automatic camera upload, thumbnails are now regularly generated, regardless of the device with which the photos were taken.
- Fixed issues with adding 2FA secured cloud storage provider
- Bug fixes and improvements

Version 2.106.992 (2021-05-10)

- Fixed issues when uploading files from external apps
- Fixed camera upload issues
- Fixed offline file issues
- Fixed issues when working with big files
- Fixed issues with thumbnail generation
- Improved performance when working with bad internet connection
- Minor bug fixes and improvements

Version 2.105.935 (2020-12-04)

- Fixed issues with adding 2FA secured cloud storage provider on pixel devices.
- Fixed issues with accessing Whisply shared files.
- Fixed issues with accessing mail.ru Hotbox.
- Minor bug fixes and improvements

Version 2.104.916 (2020-11-10)

- Files can now be downloaded to the device.
- Fixed issues with adding a cloud storage provider.
- Fixed issues with saving files from other apps.

- Fixed issues with local key files.
- Minor bug fixes and improvements

Version 2.103.895 (2020-09-29)

- Google Drive shortcuts support
- Minor bug fixes and improvements

Version 2.102.884 (2020-09-01)

- Official Android 11 support
- Improved WebDAV performance
- Minor bug fixes and improvements

Version 2.101.875 (2020-08-07)

- Fixed issues with camera upload permissions on Android 10

Version 2.100.873 (2020-08-05)

- Fixed issues with Dropbox Vault
- Fixed performance issues with Strato HiDrive and Telekom MagentaCLOUD
- Improved stability
- Minor Bugfixes and improvements

Version 2.99.838 (2020-04-18)

- Fix OneDrive Germany Authentication
- Fix storage authentication after failure
- Improved Google Drive performance
- Improved Upload stability
- Reduce memory usage for thumbnail generation
- Minor bugfixes and improvements

Version 2.98.822 (2020-04-07)

- We added LeitzCloud to our supported cloud storage provider list
- Bug fixes and improvements

Version 2.97.815 (2020-03-19)

- Bug fixes and improvements

Version 2.96.808 (2020-03-12)

- Bug fixes and improvements

Version 2.95.804 (2020-03-04)

- Improved filebrowser usability
- Bug fixes and improvements

Version 2.94.790 (2020-01-21)

- Bug fixes and improvements

Version 2.93.786 (2020-01-14)

- Bug fixes and improvements

Version 2.92.783 (2020-01-09)

- App Protection with system authentication methods
- Open office files directly from the browser
- Fixed web based storage provider authentication
- Bug fixes and improvements

Version 2.91.776 (2019-12-12)

- Bug fixes and improvements

Version 2.90.771 (2019-12-03)

- Adds IONOS HiDrive support
- Discontinued Orange Cloud support
- Improved overall performance
- Bug fixes and improvements

Version 2.89.747 (2019-10-23)

- Minor bug fixes and improvements

Version 2.88.746 (2019-10-07)

- Minor bug fixes and improvements

Version 2.87.745 (2019-09-26)

- Minor bug fixes and improvements

Version 2.86.740 (2019-09-04)

- Adds official Android 10 support
- Minor bug fixes and improvements

Version 2.85.736 (2019-08-27)

- Adds Offline Files. Make files offline available so they stay always on your device.
- Adds faster image preview if a thumbnail is already available.
- Minor bug fixes and improvements

Version 2.84.720 (2019-07-11)

- Adds thumbnails for downloaded and uploaded images
- Adds a grid view to the browser
- Adds new and beautiful file icons

- Better handling for conflicting files after editing
- Fixes issues with the Microsoft Office integration
- Minor bug fixes and improvements

Version 2.83.713 (2019-06-04)

We added Wasabi to our supported cloud storage provider list

Version 2.82.711 (2019-05-22)

- Minor bug fixes and improvements

Version 2.81.710 (2019-05-02)

- Minor bug fixes and improvements

Version 2.80.709 (2019-04-11)

- Minor bug fixes and improvements

Version 2.79.708 (2019-04-10)

- Minor bug fixes and improvements

Version 2.78.706 (2019-04-09)

We have completely reworked Boxcryptor with the following highlights:

- Faster download
- Faster upload
- Overall improved speed
- Modern user interface
- Overall improved user experience
- Improved camera upload
- Overall improved reliability

Version 2.77.687 (2018-09-06)

- Minor bug fixes and improvements

Version 2.76.673 (2018-08-03)

- Minor bug fixes and improvements

Version 2.75.662 (2018-07-20)

- Minor bug fixes and improvements

Version 2.74.661 (2018-07-12)

- Improved: Sorting of filenames containing numbers
- Improved: Detection of several file types to open files in correct app

- Fixed: Several issues during upload
- Fixed: Show notifications on Android 8
- Minor bug fixes and improvements

Version 2.73.634 (2018-05-11)

- Added: Dropbox Team Space support
- Added: Enter Sharepoint Site URL
- Minor bug fixes and improvements

Version 2.72.627 (2018-02-26)

- Added: ownCloud support
- Added: Nextcloud support
- Minor bug fixes and improvements

Version 2.71.614 (2017-12-18)

- Minor bug fixes and improvements

Version 2.70.613 (2017-12-13)

- Improved: Faster Startup
- Minor bug fixes and improvements

Version 2.69.609 (2017-11-07)

- Improved: Storage Provider Communication
- Improved: Orange Authentication
- Minor bug fixes and improvements

Version 2.68.606 (2017-09-18)

- Fixed: WebDAV credentials input

Version 2.67.605 (2017-09-18)

- Fixed: Telekom Secure Data Drive
- Minor bug fixes and improvements

Version 2.66.604 (2017-09-07)

- New: Major redesign of the user interface for creating accounts and signing in
- New: Nutstore support
- Improved: Storage provider error messages
- Minor bug fixes and improvements

Version 2.65.594 (2017-07-31)

- New: Fingerprint App Protection support
- Minor bug fixes and improvements

Version 2.64.591 (2017-07-17)

- New: Google Team Drives support
- Minor bug fixes and improvements

Version 2.63.590 (2017-07-04)

- Fixed: Local Storage Listing

Version 2.62.589 (2017-06-30)

- Minor bug fixes and improvements

Version 2.61.588 (2017-06-22)

- Improved: Camera Upload
- Minor bug fixes and improvements

Version 2.60.580 (2017-06-13)

- New: OneDrive for Business Germany support
- Fixed: Google Drive authentication
- Minor bug fixes and improvements

Version 2.59.575 (2017-04-12)

- Minor bug fixes and improvements

Version 2.58.574 (2017-04-11)

- New: Chromebook Support
- New: Chrome Tab support for Strato HiDrive
- Fixed: Chrome Tab not working on some devices
- Fixed: OneDrive upload
- Fixed: CloudMe sign in
- Fixed: Egnyte listing
- Minor bug fixes and improvements

Version 2.56.569 (2017-03-28)

- New: mail.ru Hotbox support
- New: Cancel operations in browser view
- Improved: App Unlock experience
- Improved: Network stability
- Fixed: Microsoft Office files open read-only
- Minor bug fixes and improvements

Version 2.55.568 (2017-02-27)

- New: Take a Photo directly in Boxcryptor
- New: PDF Preview
- New: Download Progress in Previewer
- New: Chrome Tab support for Provider Credentials

- Improved: Russian Texts
- Improved: Speed & Stability
- Minor bug fixes and improvements

Version 2.54.565 (2017-01-17)

- Improved: Orange Cloud support. Please re-add your account
- Fixed: Box & hubiC download
- Minor bug fixes and improvements

Version 2.53.563 (2016-12-21)

- Minor bug fixes and improvements

Version 2.52.562 (2016-12-09)

- Fixed: Files sent to Boxcryptor lost their filename when uploading

Version 2.51.561 (2016-11-25)

- Minor bug fixes and improvements

Version 2.50.560 (2016-11-25)

- Minor bug fixes and improvements

Version 2.49.559 (2016-11-17)

- Improved: Browsing experience
- Fixed: Amazon Cloud Drive issues
- Minor bug fixes and improvements

Version 2.48.557 (2016-11-03)

- New: SharePoint Online suppor
- New: Show Recent Activities
- Improved: Yandex support. Please re-add your accoun
- Improved: SD-card suppor
- Improved: PIN code handlin
- Major internal code improvement
- Minor bug fixes and improvements

Version 2.1.447.546 (2016-08-25)

- Improved: Network stability
- Fixed: mailbox.org Drive WebDAV url
- Minor bug fixes and improvements

Version 2.1.446.544 (2016-08-18)

- Improved: Dropbox support
- Fixed: OneDrive (for Business) listing of folders with many entries
- Minor bug fixes and improvements

Version 2.1.445.539 (2016-08-04)

- Fixed: When using local storage, the parent directory could get deleted on file upload

Version 2.1.444.537 (2016-07-27)

- New: Favorites
- New: Boxcryptor color
- New: "Show password" button
- Improved: Faster and more stable sign in
- Improved: Telekom MagentaCLOUD support. Please re-add your account
- Fixed: Filename and permission inheritance
- Fixed: OneDrive (for Business) shared folders access
- Minor bug fixes and improvements

Version 2.1.417.536 (2016-05-13)

- New: hubiC support
- New: Create Microsoft Office files
- Improved: Strato HiDrive support. Please re-add your account
- Removed: Barracuda Copy support
- Fixed: OneDrive (for Business) issues
- Minor bug fixes and improvements

Version 2.1.417.535 (2016-04-20)

- Fixed: OneDrive (for Business) issues
- Minor bug fixes and improvements

Version 2.1.417.533 (2016-04-06)

- Added: Set Remember Password in Settings
- Added: Change Password in Settings
- Fixed: Possible OneDrive (for Business) folder listing issues
- Minor bug fixes and improvements

Version 2.1.417.532 (2016-03-30)

- New: Full Storage Access Framework support. Save and open encrypted files from other apps
- Improved: OneDrive (for Business) support. Please re-add your OneDrive (for Business) account
- Removed: Filespots support
- Minor bug fixes and improvements

Version 2.1.417.531 (2016-02-25)

- Fixed: Telekom Mediencenter is now MagentaCLOUD
- Minor bug fixes and improvements

Version 2.1.417.530 (2016-01-25)

- Minor bug fixes and improvements

Version 2.1.417.529 (2016-01-18)

- Minor bug fixes and improvements

Version 2.1.417.528 (2015-12-23)

- Minor bug fixes and improvements

Version 2.1.417.527 (2015-12-21)

- New: Android Access Storage Framework Support
- New: Rename cloud storage providers
- Improved: SD card support
- Minor bug fixes and improvements

Version 2.1.417.520 (2015-10-21)

- Fixed: Android 6.0 Permissions
- Fixed: Box Authorization
- Minor bug fixes and improvements

Version 2.1.417.519 (2015-09-30)

- Improved: File preview
- Improved: Settings screen
- Improved: Sorting of files and folders
- Added: Fastscroll in browser
- Minor bug fixes and improvements

Version 2.1.417.517 (2015-08-18)

- Minor bug fixes and improvements

Version 2.1.417.514 (2015-06-28)

- New: Material Design User Interface
- Added: Copy.com support
- Added: Orange Cloud support
- Minor bug fixes and improvements

Version 2.1.417.510 (2015-06-17)

- Added: Automatic system proxy detection
- Added: Dropbox login using Dropbox app
- Fixed: Local Account issues
- Minor bug fixes and improvements

Version 2.1.417.508 (2014-05-20)

- Added: Amazon S3 support
- Improved: WebDAV self signed certificate support
- Improved: Login speed

- Fixed: Login screen was shown if camera upload was active
- Minor bug fixes and improvements

Version 2.1.417.506 (2015-04-29)

- Added: Amazon Cloud Drive support

Version 2.1.415.498 (2014-12-15)

- Minor bug fixes and improvements

Version 2.1.415.496 (2014-12-11)

- Minor bug fixes and improvements

Version 2.1.415.493 (2014-11-26)

- Fixed: Box upload not working
- Fixed: Rename removes .bc ending
- Minor bug fixes and improvements

Version 2.1.413.484 (2014-07-29)

- Minor bug fixes and improvements

Version 2.1.413.483 (2014-07-14)

- Fixed: Account created on Android not working on other platforms
- Fixed: Switching between Local/Boxcryptor Account
- Minor bug fixes and improvements

Version 2.1.413.479 (2014-07-08)

- Added: Automatic camera upload (requires new permission: Run at startup)
- Added: Search provider- and browserlist
- Added: Create text file
- Added: PSMail Cabinet support
- Improved: Browser Performance
- Fixed: Provider 2-Factor-Authentication not working
- Minor bug fixes and improvements

Version 2.0.411.27 (2014-04-09)

- Added: Login, browse folders and open files you have already visited without internet connection
- Added: Photo thumbnails when uploading photos
- Added: OneDrive for Business support
- Added: Storegate support
- Added: mailbox.org support
- Fixed: Some files could not be decrypted
- Minor bug fixes and improvements

Version 2.0.409.25 (2014-02-25)

- Fixed: New encrypted folder could not be read on other platforms
- Modified: Renamed SkyDrive to OneDrive
- Minor bug fixes and improvements

Version 2.0.409.24 (2014-02-20)

- Added: Sort by creation date
- Added: Google Drive support to Kindle devices
- Improved: Adding cloud provider
- Fixed: Dropbox could not be added
- Fixed: Text Editor set wrong newlines
- Removed: No longer needed permissions
- Minor bug fixes and improvements

Version 2.0.407.23 (2013-12-16)

- Fixed: Cloud providers are not stored
- Modified: Updated Box
- Minor bug fixes and improvements

Version 2.0.405.21 (2013-11-04)

- Fixed: Local account & local storage usage without Internet connection
- Minor bug fixes and improvements

Version 2.0.403.19 (2013-10-21)

- Some bug fixes

Version 2.0.403.18 (10/15/2013

- Added: Translations for German, French, Spanish, Italian and Russian
- Added: PIN unlock
- Added: Support for CloudMe
- Added: Support for Grau DataSpace
- Fixed: Google Drive limits file listing
- Minor bug fixes and improvements

Version 2.0.402.17 (2013-09-24)

- Added: Image Preview Zoom
- Improved: File Preview
- Improved: User Interface
- Fixed: WebDAV issues
- Fixed: Logout on user changes
- Fixed: PRNG crash on some devices (e.g. Samsung Galaxy S4)
- Fixed: Smaller bugs

Version 2.0.402.16 (2013-08-21)

- Improved: Login Speed up to 5x faster

- Improved: User Interface
- Fixed: Android PRNG
- Fixed: FileSpots 401 Error
- Fixed: Dialog button order on older devices
- Fixed: Smaller issues

Version 2.0.402.14 (2013-07-23)

- Added: Boxcryptor Tour
- Added: Send files to Boxcryptor
- Added: Manage Uploads
- Added: Support for Filespots
- Improved: Performance
- Improved: Design
- Improved: Help/About Section
- Fixed: Login error messages
- Fixed: Smaller bugs

Version 2.0.401.13 (2013-06-25)

- Added: Support for local accounts using key files instead of the Boxcryptor Key Server
- Added: Warning if inside Boxcryptor Classic Folder
- Fixed: Small bugs

Version 2.0.400.10 (2013-06-12)

- Fixed: Could not get device id error due to missing entry of manufacturer
- Fixed: Crash when starting settings on xlarge tablets
- Fixed: Small reported bugs

Version 2.0.400.9 (2013-06-07)

- Fixed: Wrong credentials error due to wrong password hash calculation
- Fixed: Small reported bugs

Version 2.0.400.8 (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