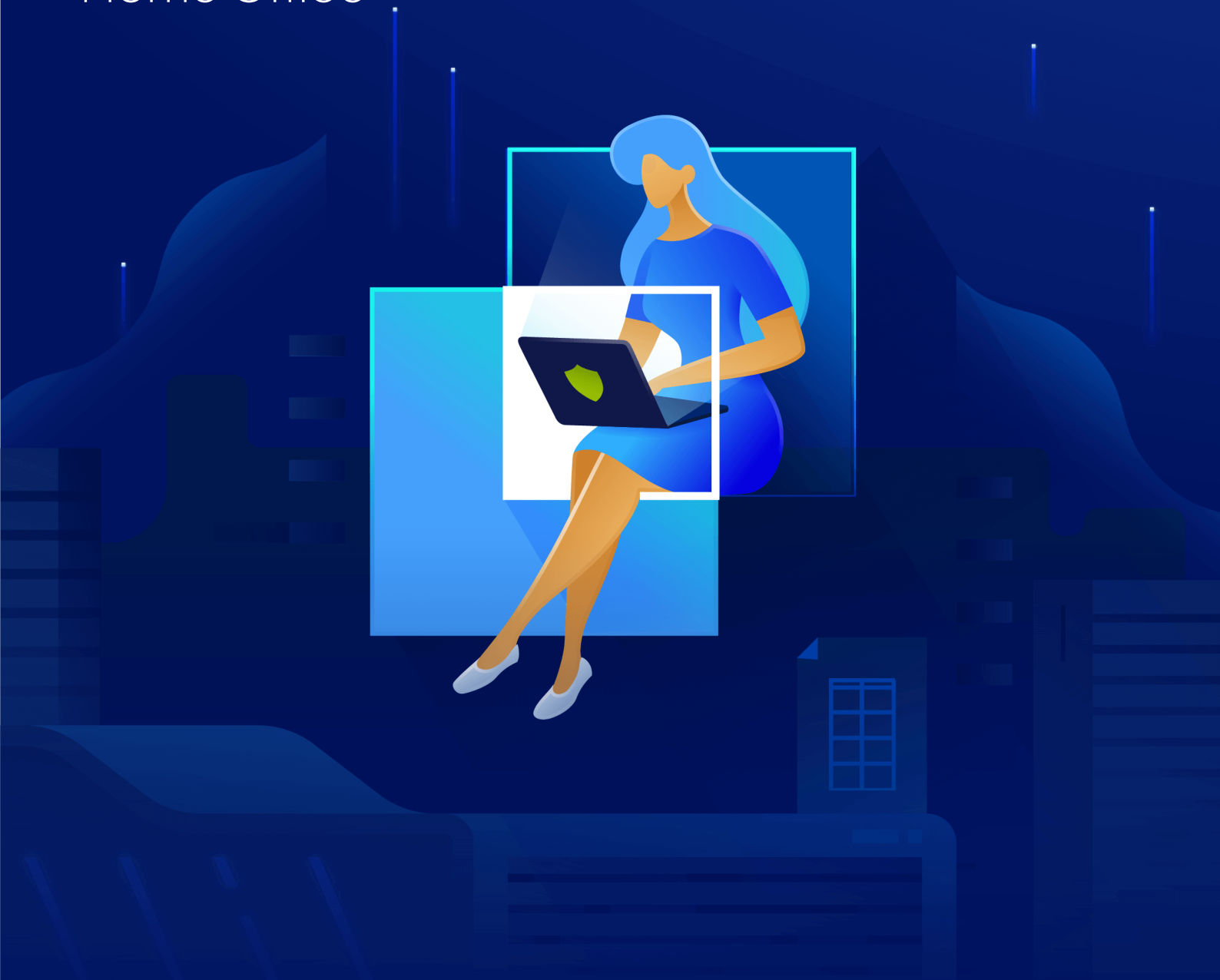
Acronis

acronis.com

# Acronis Cyber Protect

## Home Office



Benutzeranleitung für den Mac

REVISION: 09.07.2024

# Inhaltsverzeichnis

# Urheberrechtserklärung



Die Software bzw. Dienstleistung kann Code von Drittherstellern enthalten. Die Lizenzvereinbarungen für solche Drittanbieter sind in der Datei 'license.txt' aufgeführt, die sich im Stammordner des Installationsverzeichnisses befindet. Eine aktuelle Liste des verwendeten Drittanbieter-Codes sowie der dazugehörigen Lizenzvereinbarungen, die mit der Software bzw. Dienstleistung verwendet werden, finden Sie unter https://kb.acronis.com/content/7696.

# Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 sowie weitere, schwebende Patentanmeldungen.

# Einführung

## Was ist Acronis Cyber Protect Home Office?

Acronis Cyber Protect Home Office ist eine Anwendung, die alle Informationen auf Ihrem Mac schützt – das Betriebssystem, Anwendungen, Einstellungen und Ihre kompletten Daten eingeschlossen.

Um Ihren Mac zu schützen, müssen Sie zwei einfache Aktionen ausführen:

1. **Ein vollständiges Backup Ihres Macs erstellen.**
   Dadurch werden die Dateien Ihres Betriebssystems und all Ihre Daten in eine Datei gespeichert, die 'Backup' genannt wird. Sie können diese Datei in einem Storage (hier verwendeter Oberbegriff für Datenspeicher aller Art) speichern, der lokal oder im Netzwerk liegt. Oder die Datei auch in die Acronis Cloud hochladen. Weitere Details finden Sie im Abschnitt 'Backup zu einem lokalen oder Netzwerk-Storage' und 'Backup in die Acronis Cloud'.
2. **Erstellen Sie ein Acronis Boot-Medium**.
   Dabei handelt es sich um ein Wechsellaufwerk, welches entsprechende Boot-Dateien enthält. Sollte Ihr Mac einmal nicht mehr starten können, dann ermöglicht Ihnen dieses Medium, eine Wiederherstellungsumgebung von Acronis auszuführen. Sie können dann Ihr Backup verwenden, um Ihren Mac in einen fehlerfreien Zustand zurückzuversetzen. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.

Nach Ausführung dieser beiden Schritte können Sie sicher sein, dass Sie Ihr macOS reparieren und verlorene Dokumente in wenigen Minuten wiederherstellen können.

**Kernfunktionen:**

- Ausgewählte Laufwerke oder die kompletten Inhalte eines Macs zu einem lokalen oder Netzwerk-Storage oder in die Acronis Cloud sichern
- Ausgewählte Dateien und Ordner zu einem lokalen oder Netzwerk-Storage oder in die Acronis Cloud sichern
- Antivirus Protection
- Archivierung von Daten
- Online Dashboard
- Ein Acronis Boot-Medium erstellen
- macOS in der Umgebung eines Boot-Mediums wiederherstellen
- Bestimmte Dateien und Ordner unter macOS wiederherstellen

## Systemanforderungen

**Unterstützte Betriebssysteme**

- macOS Sonoma 14
- macOS Ventura 13
- macOS Monterey 12
- macOS Big Sur 11
- macOS Catalina 10.15

**Hinweis**
Mac-Maschinen mit Intel Core 2 Duo-Prozessoren werden nicht unterstützt.

**Unterstützte Dateisysteme**

- APFS
- HFS+ (inklusive Core Storage)
- FAT32
- NTFS (inkl. Boot Camp)

**Hinweis**
Sie können keine Backups zu einem Laufwerk mit NTFS-Dateisystem sichern. Es ist jedoch möglich, Daten aus einem Backup wiederherzustellen, das sich auf einem Laufwerk in einem solchen Dateisystem befindet.

**Die Anforderungen für ein Acronis Boot-Medium**

- Um ein Boot-Medium zu erstellen, können Sie ein Wechsellaufwerk verwenden, welches mit den Dateisystemen APFS oder Mac OS Extended formatiert ist und über 4,3 GB (oder mehr) freien Speicherplatz verfügt.
- Die Version von macOS Recovery muss zu der Version von macOS passen, die auf Ihrem Mac installiert ist.
- CD- und DVD-Medien werden nicht unterstützt.

**Unterstützte Speichermedien**

- Interne Laufwerke (HDD, SSD)
- SoftRAID® (wird für Backups und Wiederherstellungen von Dateien und Ordnern unterstützt)
- USB-Laufwerke
- FireWire-Laufwerke
- Thunderbolt-Laufwerke
- Netzwerk-Freigabe, NAS (ausgenommen WD My Cloud Home und WD My Cloud Home Duo)
- Acronis Cloud

**Nicht unterstützte Konfigurationen**

- Apple RAID und andere RAIDs (mit Ausnahme derjenigen, die im Abschnitt '**Unterstützte Speichermedien**' aufgeführt sind)

**Unterstützte Prozessoren**

- Apple Silicon (mit M1- oder M2-Chip)
- Intel (x86)

**Allgemeine Anforderungen**

- Sie benötigen administrative Berechtigungen, um Acronis Cyber Protect Home Office ausführen zu können.
- [Auf einem Intel-basierten Mac, außer mit macOS Big Sur 11, Monterey 12, Ventura 13 oder Sonoma 14] Wenn Ihr Mac über einen Apple T2-Chip verfügt, wählen Sie in den Einstellungen für 'Sicheres Starten' die Optionen **Mittlere Sicherheit** und **Starten von externen Medien erlauben**. Weitere Informationen dazu finden Sie unter https://support.apple.com/de-de/HT208330.
- [Auf einem Intel-basierten Mac, mit macOS Big Sur 11, Monterey 12, Ventura 13 oder Sonoma 14] Wenn Ihr Mac über einen Apple T2-Chip verfügt, wählen Sie in den Einstellungen für 'Sicheres Starten' die Optionen **Ohne Sicherheit** und **Starten von externen Medien erlauben**. Weitere Informationen dazu finden Sie unter https://support.apple.com/de-de/HT208330.

**Unterstützung für den Dunkelmodus (Dark Mode)**

Der Dunkelmodus ist ab macOS Big Sur verfügbar. Acronis Cyber Protect Home Office schaltet auf eine dunkle Benutzeroberflächendarstellung um, wenn der Dunkelmodus im macOS eingeschaltet ist.

# Acronis Cyber Protect Home Office installieren, aktualisieren oder entfernen

***So können Sie Acronis Cyber Protect Home Office installieren***

1. Laden Sie die Acronis Cyber Protect Home Office-Setup-Datei von der Acronis Website unter https://go.acronis.com/home-office herunter.
2. Klicken Sie doppelt auf die Setup-Datei von Acronis Cyber Protect Home Office (die Datei hat die Erweiterung '.dmg').
3. Klicken Sie im **Acronis Cyber Protect Home Office**-Fenster doppelt auf **Installieren Acronis Cyber Protect Home Office**.
4. Befolgen Sie die Anweisungen des Installers. Geben Sie auf Aufforderung die Administrator-Anmeldedaten ein.
5. Lesen Sie die Bedingungen der Lizenzvereinbarung sowie des 'Acronis Programm zur Kundenzufriedenheit (CEP)' und akzeptieren Sie diese.
6. Wenn Sie Acronis Cyber Protect Home Office zum ersten Mal starten, können Sie die nachfolgenden Aktionen im Fenster **Aktivierung** durchführen:

- Wenn Sie Acronis Cyber Protect Home Office aktivieren wollen, geben Sie Ihre Seriennummer ein und klicken Sie dann auf **Aktivieren**. Das Produkt wird automatisch aktiviert.
- Wenn Sie sich an Ihrem Acronis Konto anmelden wollen, klicken Sie auf **Anmelden**. Ausführlichere Informationen finden Sie im Abschnitt '"Acronis Cyber Protect Home Office aktivieren" (S. 11)'.
- Wenn Sie die Testversion starten wollen, klicken Sie auf **Testversion starten**.

Wenn auf Ihrem Mac macOS Catalina 10.15 läuft, müssen Sie der Acronis International GmbH nach der Installation Zugriff auf die Laufwerke gewähren. Dies ist erforderlich, um die Kernel-Erweiterungen zu laden, damit alle Schutzfunktionen verwendet werden können. Gehen Sie folgendermaßen vor:

1. Öffnen Sie die **Systemeinstellungen**.
2. Gehen Sie zur Registerkarte **Allgemein** des Fensters **Datenschutz & Sicherheit**.
3. Klicken Sie auf **Erlauben**, um die erscheinende Aufforderung zu akzeptieren.

Sie müssen Acronis Cyber Protect Home Office außerdem Vollzugriff auf die Festplattenlaufwerke gewähren. Auf einem Mac mit macOS Catalina 10.15 werden die Backup-, Klonen- und Schutz-Funktionalitäten ohne vollständigen Laufwerkszugriff nicht korrekt funktionieren. Auf einem Mac mit macOS Big Sur 11, Monterey 12, Ventura 13 oder Sonoma 14 werden die Backup- und Klon-Funktionalitäten ohne vollständigen Laufwerkszugriff nicht richtig funktionieren und die Schutz-Funktionalität wird komplett deaktiviert. Wenn Sie den Zugriff ermöglichen wollen, befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie aufgefordert werden, die Berechtigung 'Vollzugriff auf Festplatte' zu gewähren. Weitere Informationen dazu finden Sie unter https://kb.acronis.com/content/61832.

***So können Sie Acronis Cyber Protect Home Office aktualisieren***

Wenn die Acronis Website ein Update für Acronis Cyber Protect Home Office bereitstellt, werden Sie entsprechend benachrichtigt. Anschließend können Sie das Update herunterladen. Anschließend können Sie es über Ihre Version von Acronis Cyber Protect Home Office drüberinstallieren. All Ihre Backups und Einstellungen bleiben dabei erhalten.

Wenn Sie eine automatische Prüfung nutzen wollen, müssen Sie im Menü von Acronis Cyber Protect Home Office auf **Einstellungen** klicken und dann das Kontrollkästchen **Beim Start automatisch auf Updates prüfen** aktivieren (ist standardmäßig eingeschaltet).

Wenn Sie manuell nach Updates suchen wollen, klicken Sie im Acronis Cyber Protect Home Office-Menü auf den Befehl **Auf Updates prüfen**.

***So können Sie Acronis Cyber Protect Home Office entfernen***

1. Laden Sie die Setup-Datei von Acronis Cyber Protect Home Office von der Acronis Website herunter.
2. Klicken Sie doppelt auf die Setup-Datei von Acronis Cyber Protect Home Office (die Datei hat die Erweiterung '.dmg').

3. Klicken Sie im **Acronis Cyber Protect Home Office**-Fenster auf **Deinstallieren Acronis Cyber Protect Home Office** und bestätigen Sie Ihre Deinstallationsabsicht.
4. Geben Sie auf Aufforderung die Administrator-Anmeldedaten ein.

# Acronis Cyber Protect Home Office aktivieren

Um Acronis Cyber Protect Home Office nutzen zu können, müssen Sie dieses über das Internet aktivieren. Ohne Aktivierung können Sie das Produkt für 30 Tage mit vollem Funktionsumfang nutzen. Wenn Sie es innerhalb dieses Zeitraums nicht aktivieren, steht Ihnen anschließend nur noch die Programmfunktion 'Recovery' (Wiederherstellung) zur Verfügung. Wenn Ihr Computer zum ersten Mal mit dem Internet verbunden wird und Sie sich mit Ihrem Anmeldenamen und Kennwort an Acronis Cyber Protect Home Office anmelden, wird das Produkt automatisch aktiviert.

## Zu viele Aktivierungen

Mögliche Gründe für das 'Zu viele Aktivierungen'-Problem

- **Sie haben die maximale Anzahl der Computer, auf denen Acronis Cyber Protect Home Office installiert ist, überschritten.**

  Beispielsweise, weil Sie eine Lizenz oder eine Seriennummer für nur einen Computer haben und versuchen, Acronis Cyber Protect Home Office auf einem zweiten Computer zu installieren.

  **Lösungen:**

  - Geben Sie eine neue Seriennummer ein. Sollten Sie noch keine haben, dann können Sie diese über den integrierten Acronis Store oder über die Acronis Website erwerben.
  - Verschieben Sie die Lizenz von einem anderen Computer, auf dem das Produkt bereits aktiviert ist, zu Ihrem neuen Computer. Wählen Sie dazu denjenigen Computer aus, von dem aus Sie die Lizenz verschieben wollen. Beachten Sie, dass Acronis Cyber Protect Home Office auf diesem Computer deaktiviert wird.
- **Sie installieren macOS neu oder ändern die Hardware Ihres Computers.**

  Sie führen beispielsweise bei Ihrem Computer ein Upgrade Ihres Mainboards oder Prozessors durch. Die Aktivierung geht verloren, weil Acronis Cyber Protect Home Office Ihren veränderten Computer als neu ansieht.

  **Lösung:**

  Um Acronis Cyber Protect Home Office auf Ihrem Computer neu aktivieren zu können, wählen Sie denselben Computer aus der Liste anhand seines alten (bisherigen) Namens aus.

## Ihre Abonnementlizenzen manuell verwalten

Wenn Sie eine abonnementbasierte Version von Acronis Cyber Protect Home Office verwenden, können Sie die entsprechende(n) Lizenz(en) manuell auf der Acronis Website verwalten. Sie können Folgendes tun:

- Lizenzen zwischen Ihren Computer verschieben
- Lizenzen zwischen Ihren Konten übertragen

- Eine Lizenz von einem Computer entfernen
- Produktaktivierungskonflikte lösen (inkl. dem Problem 'Zu viele Aktivierungen')
- Neue Lizenzen kaufen

***So können Sie Lizenzen verwalten***

1. Gehen Sie zu 'https://account.acronis.com/' und melden Sie sich an Ihrem Acronis Konto an.
2. Suchen Sie im Bereich '**Produkte**' den Eintrag für 'Acronis Cyber Protect Home Office' und klicken Sie dann auf **Verwalten**.

# Informationen zur Testversion

Falls Sie Acronis Cyber Protect Home Office zuerst testen und bewerten wollen, können Sie das Produkt als kostenlose 30-tägige Testversion installieren. Nach Ablauf des Testzeitraums wird die Programmfunktionalität geblockt. Falls Sie Acronis Cyber Protect Home Office danach noch weiter verwenden wollen, müssen Sie ein Upgrade auf die Vollversion durchführen. Beachten Sie, dass die Funktion 'Laufwerk klonen' in der Testversion der Applikation deaktiviert ist.

Auf Ihrem lokalen System oder im lokalen Netzwerk gespeicherte Backups werden nach Ablauf des Testzeitraums nicht gelöscht und können mithilfe der Vollversion von Acronis Cyber Protect Home Office jederzeit wiederhergestellt werden.

Für den Testzeitraum stehen Ihnen 1000 GB Cloud-Speicherplatz zur Verfügung. Sie können diesen Speicherplatz verwenden, um Ihre Backups online zu speichern. Nach Ablauf des Testzeitraums funktioniert die Acronis Cloud noch für 30 Tage im Modus 'Nur Recovery'. Nach Ablauf dieses Zeitraums können Sie den Acronis Cloud Service nicht mehr verwenden und all Ihre Daten werden gelöscht.

***So können Sie die Testversion installieren***

Um die Testversion verwenden zu können, müssen Sie das Produkt zuerst installieren und dann im Fenster **Activation** auf **Testversion starten** klicken. Details finden Sie im Abschnitt 'Acronis Cyber Protect Home Office installieren, aktualisieren oder entfernen'.

***So können Sie ein Upgrade auf die Vollversion des Produkts durchführen***

1. Erwerben Sie die Vollversion auf der Acronis Website: https://go.acronis.com/mac/getfullversion.
2. Öffnen Sie Acronis Cyber Protect Home Office.
3. Klicken Sie in der Acronis Cyber Protect Home Office-Menüleiste auf den Befehl **Seriennummer eingeben**.
4. Geben Sie die vollständige Seriennummer in das entsprechende Eingabefeld ein und klicken Sie dann auf **Aktivieren**.

# Acronis Programm zur Kundenzufriedenheit (CEP)

Das Acronis Programm zur Kundenzufriedenheit (CEP) ermöglicht Acronis Kunden, Einfluss auf die Funktionen, das Design und die Entwicklung von Acronis Produkten zu nehmen. Das Programm ermöglicht Ihnen, uns mit verschiedenen Informationen zu versorgen, z.B. über die Hardware-Konfiguration physischer Computer oder virtueller Maschinen, über die am häufigsten (oder seltensten) verwendeten Funktionen und die Probleme, mit denen Sie sich konfrontiert sehen. Auf Basis dieser Informationen wollen wir die Produkte und Funktionen von Acronis verbessern, die Sie am häufigsten nutzen.

***So können Sie am Acronis Programm zur Kundenzufriedenheit (CEP) teilnehmen oder dieses wieder verlassen***

1. Klicken Sie im Menü Acronis Cyber Protect Home Office auf den Befehl **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen für **Am Acronis Programm zur Kundenzufriedenheit (CEP) teilnehmen**, um das Programm wieder zu verlassen.

Wenn Sie sich für eine Teilnahme entscheiden, werden jede Woche entsprechende technische Informationen automatisch eingeholt. Es werden keine persönlichen Daten, wie z.B. Namen, Adressen, Telefonnummern oder Tastatureingaben gesammelt. Die Teilnahme am Programm zur Kundenzufriedenheit (CEP) ist freiwillig. Die Ergebnisse dieses Programms sind ausschließlich dazu gedacht, die Software zu verbessern, dessen Funktionalität zu erweitern und die Erwartungen unserer Kunden zukünftig noch besser erfüllen zu können.

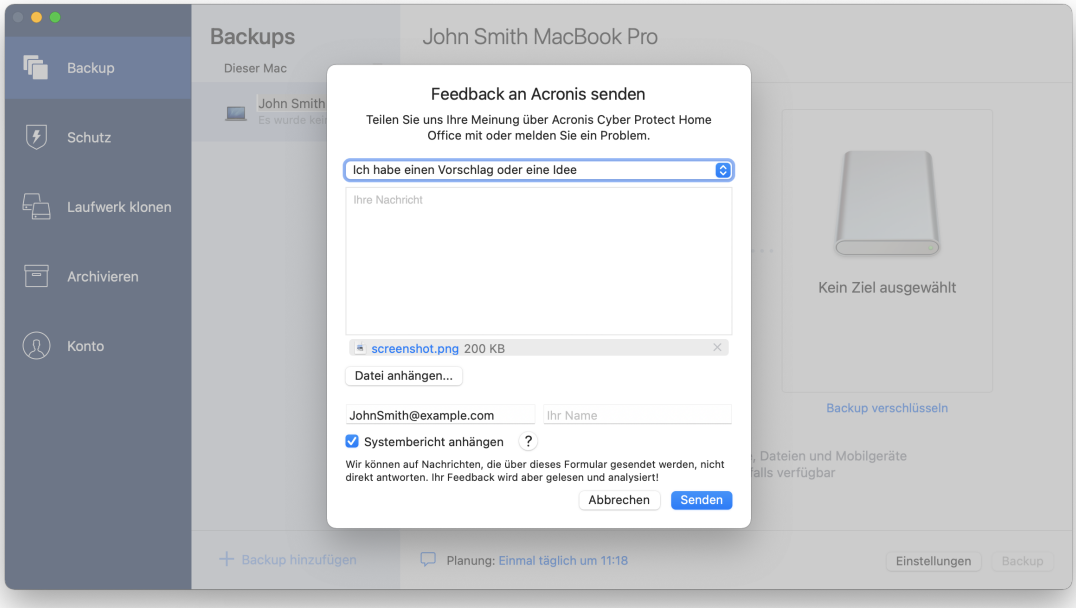
# Feedback an Acronis senden

Wir verbessern unsere Produkte und Dienste regelmäßig, indem wir sie funktioneller, zuverlässiger und schneller machen. Sie können uns über das Rückmeldungsformular Unannehmlichkeiten oder fehlerhafte Funktionen mitteilen, die wir zur Verbesserung von Acronis Cyber Protect Home Office beheben sollen. Bitte geben Sie uns einige Ihrer Minuten, um uns mitzuteilen, was Sie von unserem Produkt halten, um eine neue Funktion vorzuschlagen oder ein Problem zu melden. Alle Rückmeldungen werden von uns gelesen und analysiert.

**Hinweis**
Wir können jedoch nicht auf alle Rückmeldungen antworten. Sollten Sie Unterstützung für Acronis Cyber Protect Home Office benötigen, dann wenden Sie sich an den entsprechenden Support.

**So können Sie ein Feedback an Acronis** senden

1. Klicken Sie im Acronis Cyber Protect Home Office-Menü auf den Befehl **Feedback senden**. Daraufhin wird das Rückmeldungsformular geöffnet.




2. Wählen Sie einen Grund für Ihre Rückmeldung aus der Liste aus.
3. Geben Sie Ihre Nachricht ein.
4. Geben Sie Ihren Namen und Ihre E-Mail-Adresse an.
5. [Optionaler Schritt] Acronis Cyber Protect Home Office hängt standardmäßig ein Bildschirmfoto (Screenshot) des Konsolenfensters an. Falls Sie der Meinung sind, dass uns der Screenshot nicht helfen wird, Ihr Problem zu untersuchen bzw. Ihre Aussage zu verstehen, können Sie es auch löschen.
6. [Optionaler Schritt] Sie können eine Datei und einen Acronis Systembericht anhängen.

   Ein Acronis Systembericht enthält diverse technische Informationen (einschließlich Informationen über Ihre Hardware-Konfiguration, die macOS-Version, das Systemprotokoll sowie das Ereignisprotokoll von Acronis Cyber Protect Home Office) und Ihre Backup-Einstellungen.

   **Hinweis**
   Ein Acronis Systembericht enthält keine persönlichen Daten (wie z.B. Namen, Adressen, Telefonnummern) und es werden auch keine Tastatureingaben gesammelt.

   Wir empfehlen Ihnen, einen Systembericht anzuhängen, wenn Sie mit einem ernsthaften Problem konfrontiert wurden (beispielsweise, wenn Acronis Cyber Protect Home Office nicht mehr reagiert).
7. Klicken Sie auf **Senden**.

# Applikationseinstellungen

**Hinweis**
Bestimmte Programmfunktionen sind in der von Ihnen verwendeten Edition möglicherweise nicht verfügbar.

Im Fenster 'Einstellungen' finden Sie die allgemeinen Konfigurationseinstellungen von Acronis Cyber Protect Home Office. Sie können Sie das Fenster öffnen:

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Klicken Sie im Menü Acronis Cyber Protect Home Office auf den Befehl **Einstellungen**.

Folgende Einstellungen sind in der Registerkarte **Allgemein** verfügbar:

- **Backup, wenn Ihr Mac im Power Nap-Modus ist**
  Backups können ausgeführt werden, wenn Ihr Mac im Ruhezustand ist. Weitere Informationen finden Sie im Abschnitt 'Planung'.
- **Beim Start automatisch auf Updates prüfen**
  Details finden Sie im Abschnitt 'Acronis Cyber Protect Home Office installieren, aktualisieren oder entfernen'.
- **Am Acronis Programm zur Kundenzufriedenheit (CEP) teilnehmen**
  Weitere Informationen finden Sie im Abschnitt 'Acronis Programm zur Kundenzufriedenheit (CEP)'.
- **Benachrichtigungen in der Mitteilungszentrale anzeigen**
  Weitere Informationen finden Sie im Abschnitt 'Benachrichtigungen'.
- **Personalisierte Angebote anzeigen**
  Aktivieren Sie dieses Kontrollkästchen, um personalisierte Angebote über Produkte und Funktionen zu erhalten.

Folgende Einstellungen sind in der Registerkarte **Energiesparmodus** verfügbar:

- **Kein Backup, wenn Computer im Akkubetrieb ist**
  Weitere Informationen finden Sie im Abschnitt 'Energieeinstellungen für Notebooks und Tablets'.

Folgende Einstellungen sind in der Registerkarte **WLAN-Verbindungen** verfügbar:

- **Backup nur bei ausgewählten WLAN-Verbindungen**
  Wenn sich das Gerät mit einem hier nicht ausgewählten Netzwerk verbindet, werden alle Cloud Backups pausiert. Die pausierten Backups werden fortgesetzt, sobald wieder eine Verbindung mit einem ausgewählten Netzwerk besteht. Weitere Informationen finden Sie im Abschnitt 'WLAN-Verbindungen für Backups in die Acronis Cloud'.

# Tastaturkürzel

Sie können Tastaturkürzel (auch Tastenkombinationen genannt) verwenden, um bequemer und schneller durch die Benutzeroberfläche von Acronis Cyber Protect Home Office zu navigieren. Ein Tastaturkürzel wird ausgeführt, wenn Sie eine Kombination aus zwei oder mehr Tasten gleichzeitig drücken. Einige der Tastaturkürzel von Acronis Cyber Protect Home Office werden im im Applikationsmenü angezeigt. In den Menüs sind einige Tastenbezeichnungen durch folgende Symbole ersetzt:

| Schlüsselname | Symbol |
|---|---|
| Befehl | ⌘ |
| Option | ⌥ |
| Shift (Umschalttaste) | ⇧ |

Tastaturkürzel in Acronis Cyber Protect Home Office:

| Tastaturkürzel | Beschreibung |
|---|---|
| Befehlstaste + U | Auf Produkt-Updates prüfen |
| Shift + Befehlstaste + E | Seriennummer eingeben |
| Befehlstaste + , | Fenster 'Applikationseinstellungen' öffnen |
| Shift + Befehlstaste + L | An Ihrem Konto anmelden |
| Shift + Befehlstaste + O | Von Ihrem Konto abmelden |
| Befehlstaste + N | Neues Backup erstellen |
| Befehlstaste + 1 | Den Bereich **Backup** öffnen |
| Befehlstaste + 2 | Den Bereich **Schutz** öffnen |
| Befehlstaste + 3 | Den Bereich **Laufwerk klonen** öffnen |
| Befehlstaste + 4 | Den Bereich **Archivieren** öffnen |
| Befehlstaste + 5 | Den Bereich **Konto** öffnen |
| **Bereich 'Backup'** | |
| Befehlstaste + S | Dialog 'Backup-Quelle' öffnen |
| Befehlstaste + D | Den Dialog 'Backup-Ziel' öffnen |
| Befehlstaste + Shift + S | Den Dialog 'Backup-Einstellungen' öffnen |
| **Der Bereich 'Laufwerk klonen'** | |

| Tastaturkürzel | Beschreibung |
|---|---|
| Befehlstaste + S | Den Dialog 'Quelle für die Klonen-Aktion' öffnen |
| Befehlstaste + D | Den Dialog 'Ziel für die Klon-Aktion' öffnen |
| **Bereich 'Archivieren'** | |
| Befehlstaste + O | Den Dialog 'Dateiauswahl' öffnen, um Dateien zu einem Archiv hinzuzufügen |
| Befehlstaste + D | Den Dialog 'Archiv-Ziel' öffnen |
| Befehlstaste + I | Ein Fenster mit einem Tutorial zur Archivierung öffnen |
| Befehlstaste + Shift + S | Den Dialog mit den Archivierungseinstellungen öffnen |

# Integration in die Touch Bar

Seit den Modellen 2016 gibt es auf dem 15-Zoll MacBook Pro und dem 13-Zoll MacBook Pro mit vier Thunderbolt 3-Anschlüssen einen speziellen Interaktionsbereich im oberen Teil der Tastatur: die sogenannte Touch Bar. Die Touch Bar zeigt passende Steuerelemente in Abhängig davon an, welches Fenster gerade aktiv ist oder an welcher Aufgabe Sie gerade arbeiten. Diese Technologie vereinfacht die Interaktion mit der Benutzeroberfläche und ermöglicht es, eine Vielzahl von Aktionen durchzuführen. Beispiele: auf Schaltflächen klicken, zwischen Webseiten wechseln, die Suche verwenden, Textformatierung ändern oder Systemsteuerungsbefehle des Macs verwenden. Weitere Informationen zur Touch Bar finden Sie auch auf der Apple Website: https://support.apple.com/de-de/HT207055.

Acronis Cyber Protect Home Office unterstützt die Funktionalität der Touch Bar. Sie können mit der Touch Bar zwischen verschiedenen Bereichen der Applikation wechseln, Backups konfigurieren, Daten wiederherstellen und andere Aktionen durchführen. Wenn Sie beispielsweise ein Backup aus der Liste auswählen, sieht die Touch Bar folgendermaßen aus:


Die **Esc**-Schaltfläche und die rechts danebenliegenden Symbole sind Systemsteuerungsbefehle des Macs. Im linke Teil sind Symbole zur Navigation zwischen verschiedenen Abschnitten von Acronis Cyber Protect Home Office enthalten:

| Symbol | Beschreibung |
|---|---|
|  | Backup |
|  | Laufwerk klonen |
|  | Archivieren |
|  | Schutz |
|  | Konto |

Die Steuerelemente, die sich auf das aktuelle Fenster beziehen, befinden sich im zentralen Teil. In diesem Beispiel können Sie die Quelle, das Ziel und die Einstellungen (  ) für das Backup ändern und das Backup starten.

Sie können mit den Touch Bar-Symbolen auch ein neues Backup oder Archiv erstellen:

| Symbol | Beschreibung |
|---|---|
|  | Ein neues Backup erstellen |
|  | Ein neues Archive erstellen oder einem vorhandenen weitere Dateien hinzufügen |

# Technischer Support

Falls Sie Unterstützung für Ihr Produkt von Acronis benötigen, gehen Sie zu https://www.acronis.com/support/.

Sie können für all Ihre registrierten Software-Produkte von Acronis jederzeit Updates von unserer Website herunterladen, nachdem Sie sich an Ihrem **Konto** (unter https://account.acronis.com/) angemeldet und Ihr Produkt registriert haben. Siehe auch '**Acronis Produkte auf der Website registrieren**' (https://kb.acronis.com/content/4834) und '**Benutzeranleitung zur Acronis Website**' (https://kb.acronis.com/content/8128).

# Zwei-Faktor-Authentifizierung (2FA)

Wenn die Zwei-Faktor-Authentifizierung eingerichtet ist, müssen Sie Ihr Kennwort (den ersten Faktor) und einen Einmalcode (den zweite Faktor) eingeben, um sich am Online Dashboard anmelden zu können. Der Einmalcode, der auch Einmalkennwort genannt wird, wird von einer Authenticator-App generiert, die auf Ihrem Smartphone oder einem anderen Gerät, das Ihnen gehört, installiert werden muss. Selbst wenn jemand Ihre normalen Anmeldedaten herausfinden sollte, kann diese Person sich nicht anmelden, wenn sie keinen Zugriff auf Ihr Zweit-Faktor-Geräte hat.

## Voraussetzungen

Stellen Sie vor der Aktivierung der Zwei-Faktor-Authentifizierung (2FA) sicher, dass Sie eine kompatible Version installiert haben. Die 2FA ist mit folgenden Versionen kompatibel:

- Acronis Cyber Protect Home Office Build 40713 und höher.
  So können Sie die Build-Nummer überprüfen:
  Wählen Sie im Menü von Acronis Cyber Protect Home Office die Option **Über Acronis Cyber Protect Home Office**.

- Acronis Mobile für iOS, App-Version 6.2 und höher.
- Acronis Mobile für Android, App-Version 6.2 und höher.

***So können Sie die Zwei-Faktor-Authentifizierung für Ihr Konto einrichten***

1. Öffnen Sie das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Klicken Sie auf die Registerkarte **Konto**. Der Bereich **Zwei-Faktor-Authentifizierung (2FA)** wird im Fenster **Konto** angezeigt.
3. Aktivieren Sie die Zwei-Faktor-Authentifizierung für Ihr Konto über den Umschalter. Das Fenster **Zwei-Faktor-Authentifizierung einrichten (2FA)** wird angezeigt.
4. Installieren Sie eine Authenticator-App auf Ihrem Mobilgerät.

   Beispiele für Authenticator-Apps:

   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
5. Scannen Sie den QR-Code mit Ihrer Authenticator-App und geben Sie dann den 6-stelligen Code ein, der in der Authenticator-App im Fenster **Zwei-Faktor-Authentifizierung einrichten (2FA)** angezeigt wird.
6. Klicken Sie auf **Weiter**. Es werden Anweisungen angezeigt, wie Sie den Zugriff auf Ihr Konto wiederherstellen können, wenn Sie Ihr 2FA-Gerät verloren oder die Authenticator-App deinstalliert haben sollten.
7. Speichern oder drucken Sie die PDF-Datei aus.

**Hinweis**
Bewahren Sie diese Informationen an einem sicheren Ort auf oder drucken Sie diese zur späteren Verwendung aus. Dies ist der beste Weg, um Ihren Zugriff wiederherzustellen.

***So können Sie sich mit einer 2FA anmelden***

1. Melden Sie sich mit Ihren Anmeldedaten für Acronis an.

   Das Fenster **Zwei-Faktor-Authentifizierung** wird geöffnet.
2. Geben Sie den sechsstelligen Code ein, der in Ihrer Authenticator-App angezeigt wird.

**Wichtig**
Wenn der Code korrekt ist, aber nicht funktioniert, stellen Sie sicher, dass die Uhrzeit in der Authenticator-App mit Ihrem Gerät synchronisiert ist.

3. Klicken Sie auf **Anmelden**.

***So können Sie sicherstellen, dass Sie Ihre 2FA wiederherstellen können***

- Speichern oder drucken Sie die PDF-Datei, die einen alphanumerischen Code enthält, der als Ersatz für den QR-Code verwendet werden kann.
- Erstellen Sie ein Backup des Authenticator-Kontos, sofern die Mobilgeräte-App dies unterstützen sollte.
- Verwenden Sie eine Mobilgeräte-App, die Konten unterstützt.

***So können Sie die Zwei-Faktor-Authentifizierung (2FA) auf einem neuen Gerät wiederherstellen***

Wenn Sie Zugriff auf die zuvor eingerichtete Authentifizierungs-App für Mobilgeräte haben:

1. Installieren Sie eine Authenticator-App auf Ihrem neuen Gerät.
2. Verwenden Sie die PDF-Datei, die Sie beim Einrichten der Zwei-Faktor-Authentifizierung (2FA) auf Ihrem Gerät gesichert haben. Diese Datei enthält den 32-stelligen Code, den Sie in der Authenticator-App eingeben müssen, um die Authenticator-App erneut mit Ihrem Acronis Konto verknüpfen zu können.
3. Wenn Sie es beim Einrichten versäumt haben, die PDF-Datei zu sichern:
   a. Klicken Sie auf **2FA zurücksetzen** und geben Sie das Einmalkennwort ein, das in der Authenticator-App für Mobilgeräte angezeigt wird.
   b. Folgen Sie den Bildschirmanweisungen.

Wenn Sie keinen Zugriff auf die zuvor eingerichtete Authenticator-App für Mobilgeräte haben:

**Variante 1**: Verwenden Sie die gespeicherte PDF-Datei, um ein neues Gerät zu verknüpfen. Der Standardname der Datei lautet cyberprotect-2fa-backupcode.pdf.

**Variante 2**: Einige Authenticator-Apps (wie etwa Authy) bieten die Möglichkeit, ein Backup der 2FA-Konfigurationen zu erstellen. Sie können die 2FA später aus diesem Backup auf einem anderen bzw. neuen Gerät wiederherstellen. Installieren Sie dazu die gleiche Authenticator-Applikation auf dem entsprechenden Gerät, melden Sie sich mit demselben Authenticator-App-Konto an und stellen Sie die 2FA-Konfiguration aus diesem Authenticator-App-Backup wieder her.

**Variante 3**: Einige Authenticator-Apps (wie etwa die von Microsoft) bieten die Möglichkeit, ein Wiederherstellungskonto hinzuzufügen. Sie können die 2FA-Konfiguration später auf einem neuen Gerät wiederherstellen, indem Sie sich einfach mit dem Wiederherstellungskonto anmelden. Weitere Informationen finden Sie unter support.microsoft.com.

# Backup

## Grundlegende Konzepte

***Backup und Recovery***

Der Begriff **Backup** bezieht sich auf die Erstellung von Datenkopien, damit diese dazu verwendet werden können, die ursprünglichen Daten nach einem Datenverlust **wiederherzustellen**.

Backups haben in erster Linie zwei Funktionen:

- Um ein Betriebssystem wiederherzustellen, wenn es beschädigt ist oder nicht mehr starten kann. Dieser Prozess wird auch 'Disaster Recovery' genannt. Informationen darüber, wie Sie Ihren Mac vor einem Desaster schützen können, finden Sie im Abschnitt 'Backup zu einem lokalen oder Netzwerk-Storage'. , Backup in die Acronis Cloud .
- Um bestimmte Dateien und Ordner wiederherzustellen, nachdem diese versehentlich gelöscht oder beschädigt wurden.

**Recovery-Methoden:**

- Ein **Vollständiges Recovery** kann zum ursprünglichen oder einem neuen Speicherort durchgeführt werden.
  Wird der ursprüngliche Speicherort ausgewählt, so werden die Daten an diesem Speicherort durch die Daten aus dem Backup vollständig überschrieben. Wird ein neuer Speicherort ausgewählt, so werden die Daten aus dem Backup einfach nur zu diesem neuen Speicherort kopiert.
- Ein **Inkrementelles Recovery** kann nur zum ursprünglichen Speicherort und nur aus einem Cloud Backup durchgeführt werden. Bevor die Wiederherstellung startet, werden die Dateien am ursprünglichen Speicherort mit den Dateien im Backup anhand von Dateiattributen (wie Dateigröße und letztes Änderungsdatum) verglichen. Dateien, die nicht übereinstimmen, werden als 'wiederherzustellen' gekennzeichnet, während die übrigen Dateien bei der Wiederherstellung übersprungen werden. Anders als bei der vollständigen Wiederherstellung stellt Acronis Cyber Protect Home Office dabei nur Dateien wieder her, die seit dem Backup verändert wurden. Mit dieser Methode lässt sich bei Wiederherstellungen aus der Acronis Cloud die Wiederherstellungszeit und über das Internet übertragene Datenmenge deutlich reduzieren.

***Backup-Versionen***

Eine Backup-Version wird während einer Backup-Aktion erstellt. Eine Version repräsentiert einen Zeitpunkt, zu dem ein System bzw. Daten wiederhergestellt (im Sinne von 'zurückversetzt') werden kann bzw. können. Die erste Backup-Version enthält alle Daten, die für das Backup ausgewählt wurden. Die zweite Version und die nachfolgenden Versionen enthalten nur solche Datenänderungen, die seit der letzten Backup-Version aufgetreten sind. Alle Backup-Versionen werden in einer einzelnen Backup-Datei gespeichert.

***Format der Backup-Datei***

Wenn Sie ein Backup Ihres Macs zu einem lokalen Storage oder einem Speicherplatz im Netzwerk erstellen, speichert Acronis Cyber Protect Home Office die Backup-Daten im proprietären .tib- oder .tibx-Format – und verwendet dabei eine Kompression. Daten aus .tib- oder .tibx-Backup-Dateien können nur mit Acronis Cyber Protect Home Office wiederhergestellt werden.

Wenn Sie ein Backup Ihres Macs in die Acronis Cloud erstellen, speichert Acronis Cyber Protect Home Office Ihre Daten 'wie vorliegend'. Sie können Ihre Daten auf jedem Mac-Computer, der eine Internetverbindung hat, über das Produkt oder die Acronis Cloud wiederherstellen.

***Planung***

Damit Ihre Backups auch wirklich hilfreich sind, sollten diese so aktuell wie möglich sein. Planen Sie Ihre Backups, um sie regelmäßig auszuführen.

***Backup-Aufbewahrungsregeln***

Bei jeder Ausführung einer Backup-Aktion, egal ob manuell oder per Planung, erstellt Acronis Cyber Protect Home Office am jeweiligen Backup-Speicherort eine neue Backup-Version. Damit veraltete Backup-Versionen automatisch gelöscht werden, können Sie bestimmte Backup-Aufbewahrungsregeln festlegen. Weitere Informationen finden Sie im Abschnitt 'Backups, Backup-Versionen und Replikate bereinigen'.

# Was Sie per Backup sichern können und was nicht

Die nachfolgende Tabelle illustriert, was Sie sichern können - und wohin.

| | **Backup-Ziele** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Interne Laufwerke (HDD, SSD, RAID) | Acronis Cloud | USB-Laufwerke | Thunderbolt | AirPort Time Capsule | Netzwerk-Freigabe, NAS | CD, DVD | FTP-Server |
| Interne Laufwerke (HDD, SSD) | + | + | + | + | + | + | - | - |
| USB-Laufwerke | + | + | + | + | + | + | - | - |
| FireWire-Laufwerke | + | + | + | + | + | + | - | - |
| Thunderbolt | + | + | + | + | + | + | - | - |
| Fusion Drive | + | + | + | + | + | + | - | - |
| Festplatten, die mit FileVault 2 geschützt sind | + | + | + | + | + | + | - | - |
| Festplattenlaufwer | + | + | + | + | + | + | - | - |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ke, auf denen Boot Camp installiert ist | | | | | | | | |
| Bestimmte Dateien | + | + | + | + | + | + | - | - |
| SoftRAID | + | + | + | + | + | + | - | - |
| Andere RAIDs | - | - | - | - | - | - | - | - |
| Einzelne Volumes (Partitionen) | - | - | - | - | - | - | - | - |
| CD, DVD | - | - | - | - | - | - | - | - |
| APM-Laufwerke | - | - | - | - | - | - | - | - |

# Backup zu einem lokalen oder Netzwerk-Storage

**Hinweis**
Bestimmte Programmfunktionen sind in der von Ihnen verwendeten Edition möglicherweise nicht verfügbar.

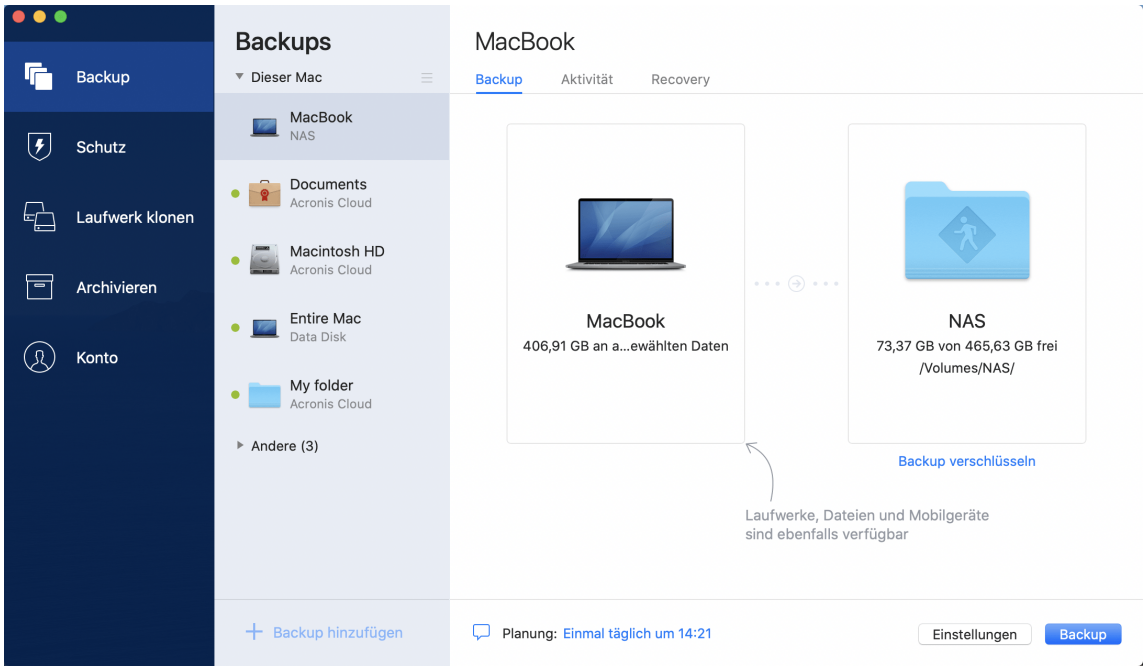
1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Gehen Sie folgendermaßen vor:
   - Überspringen Sie diesen Schritt, falls dies Ihr erstes Backup ist.
   - Sollten Sie bereits ein Backup haben und stattdessen ein neues erstellen wollen, dann klicken Sie im unteren Bereich der Backup-Liste auf **Backup hinzufügen**.

     **Hinweis**
     Klicken Sie zum Löschen eines Backups mit der rechten Maustaste auf dieses und wählen Sie anschließend den Befehl **Löschen**. Das Backup wird daraufhin aus der Liste entfernt und die entsprechenden Backup-Dateien sowie die Dateien des Backup-Replikats werden dauerhaft aus dem Backup Storage gelöscht. Diese Dateien können auf keinen Fall mehr wiederhergestellt werden.
3. Klicken Sie auf das Symbol für 'Backup-Quelle' und bestimmen Sie, was gesichert werden soll:
   - **Kompletter Mac**

     Wenn Sie diese Option auswählen, wird Acronis Cyber Protect Home Office alle vorhandenen internen Festplattenlaufwerke im 'Laufwerk-Modus' sichern. Dieses Backup enthält dann das Betriebssystem, alle installierten Programme, alle Systemeinstellungen und all Ihre persönlichen Daten (Fotos, Musikdateien und Dokumente eingeschlossen).
   - **Laufwerke**
   - **Dateien und Ordner**

**Wichtig**
Wenn Sie Daten sichern wollen, die über einen Drittanbieter-Service-Provider mit der Cloud synchronisiert werden, müssen die entsprechenden Daten zusätzlich auch lokal gespeichert werden. Wenn die Dateien oder Ordner nur in der Cloud gespeichert werden, werden Sie nur deren lokale Platzhalter sehen. Platzhalter haben meist ein Cloud-Symbol und sind zudem deutlich kleiner. Wenn Sie Quelldateien für ein Backup auswählen, müssen Sie die lokal gespeicherten Dateien und nicht die Platzhalter auswählen. Wenn der entsprechende Cloud Service Ihre Daten nicht lokal speichert, können diese nicht per Backup gesichert und daher auch nicht aus diesem wiederhergestellt werden.

- **Mobilgerät**
  Weitere Informationen finden Sie im Abschnitt 'Mobilgeräte per Backup sichern'.
- **Zu beglaubigende Dateien**
  Weitere Details finden Sie im Abschnitt 'Notarized Backup'.
- **NAS-Gerät** (sofern verbunden)




4. Klicken Sie auf das Symbol für das Backup-Ziel, bestimmen Sie den Speicherort für die Backup-Datei und klicken Sie dann auf **OK**. Sollte der Speicherort nicht aufgeführt sein, können Sie auf **Durchsuchen** klicken, um den Speicherort über den Verzeichnisbaum des Systems auszuwählen.
   Wenn Sie ein NAS-Gerät haben, wird dieses automatisch erkennt und zusammen mit den anderen Speicherorten in der Liste angezeigt.
5. [Optionaler Schritt] Konfigurieren Sie die 'Erweiterten Einstellungen'. Sie können:
   - Die Backup-Planung unter **Einstellungen** –> **Planung** konfigurieren. Weitere Informationen finden Sie im Abschnitt 'Planung'.

- Definieren Sie die Backup-Aufbewahrungsregeln unter **Einstellungen** –> **Bereinigung**. Weitere Informationen finden Sie im Abschnitt 'Backups, Backup-Versionen und Replikate bereinigen'.
- Ihr Backup per Kennwort und Verschlüsselung unter **Einstellungen** –> **Verschlüsselung** schützen. Weitere Details finden Sie im Abschnitt 'Backup-Verschlüsselung'.
- Dateien und Ordner manuell unter **Einstellungen** –> **Ausschlusskriterien** ausschließen. Weitere Details finden Sie im Abschnitt 'Elemente vom Backup ausschließen'.
- Sie können die Backup-Versuche unter **Einstellungen** —> **Fehlerbehandlung** konfigurieren.

6. Wenn Sie alle Einstellungen konfiguriert haben und bereit zum Starten eines Backups sind, dann klicken Sie auf **Backup**.

Um Ihren Mac aus einem Acronis Cyber Protect Home Office Backup wiederherstellen zu können, benötigen Sie ein Acronis Boot-Medium. Sollten Sie noch keines haben, dann erstellen Sie es. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.

# Backup in die Acronis Cloud

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Gehen Sie folgendermaßen vor:
   - Überspringen Sie diesen Schritt, falls dies Ihr erstes Backup ist.
   - Sollten Sie bereits ein Backup haben und stattdessen ein neues erstellen wollen, dann klicken Sie im unteren Bereich der Backup-Liste auf das Plus-Zeichen (+).

     **Hinweis**
     Klicken Sie zum Löschen eines Backups mit der rechten Maustaste auf dieses und wählen Sie anschließend den Befehl **Löschen**. Das Backup wird daraufhin aus der Liste entfernt und die entsprechenden Backup-Dateien werden dauerhaft aus dem Backup Storage gelöscht. Diese Dateien können auf keinen Fall mehr wiederhergestellt werden.

3. Klicken Sie auf das Symbol für 'Backup-Quelle' und bestimmen Sie, was gesichert werden soll:
   - **Kompletter Mac**
     Wenn Sie diese Option auswählen, wird Acronis Cyber Protect Home Office alle vorhandenen internen Festplattenlaufwerke im 'Laufwerk-Modus' sichern. Dieses Backup enthält dann das Betriebssystem, alle installierten Programme, alle Systemeinstellungen und all Ihre persönlichen Daten (Fotos, Musikdateien und Dokumente eingeschlossen).
   - **Laufwerke**
   - **Dateien und Ordner**

**Wichtig**

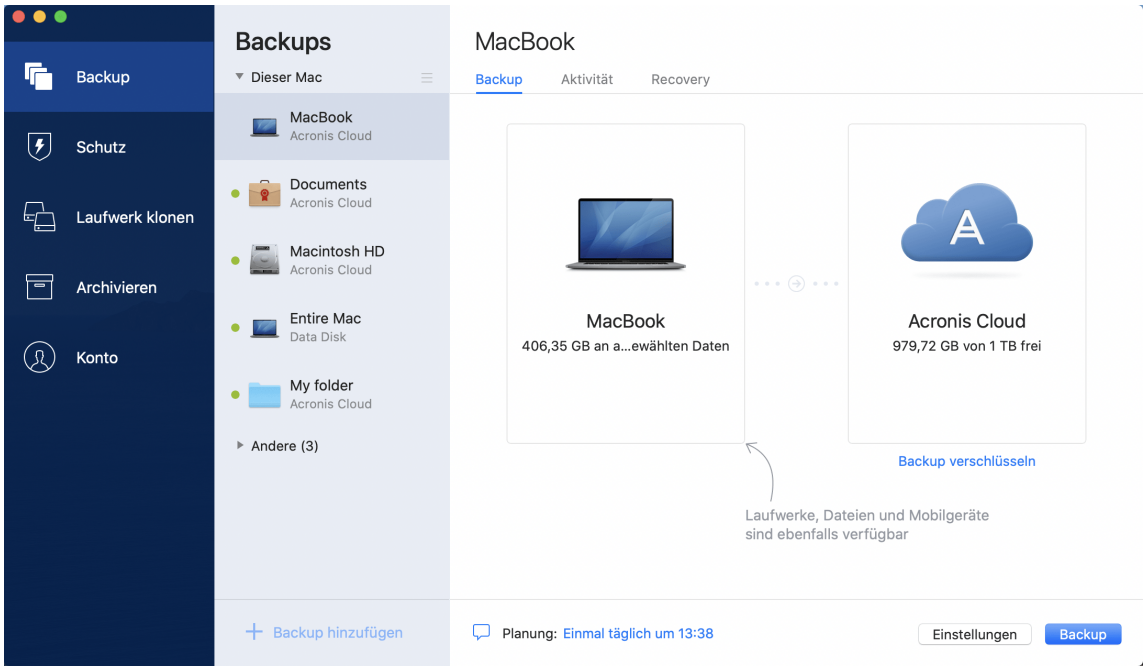
Wenn Sie Daten sichern wollen, die über einen Drittanbieter-Service-Provider mit der Cloud synchronisiert werden, müssen die entsprechenden Daten zusätzlich auch lokal gespeichert werden. Wenn die Dateien oder Ordner nur in der Cloud gespeichert werden, werden Sie nur deren lokale Platzhalter sehen. Platzhalter haben meist ein Cloud-Symbol und sind zudem deutlich kleiner. Wenn Sie Quelldateien für ein Backup auswählen, müssen Sie die lokal gespeicherten Dateien und nicht die Platzhalter auswählen. Wenn der entsprechende Cloud Service Ihre Daten nicht lokal speichert, können diese nicht per Backup gesichert und daher auch nicht aus diesem wiederhergestellt werden.

- **Mobilgerät**

  Weitere Informationen finden Sie im Abschnitt 'Mobilgeräte per Backup sichern'.
- **Cloud Service**

  Wird verwendet, um Microsoft 365-Daten zu sichern.
- **Zu beglaubigende Dateien**

  Weitere Details finden Sie im Abschnitt 'Notarized Backup'.
- NAS-Gerät (sofern verbunden)




4. Klicken Sie auf das Symbol für 'Backup-Ziel', wählen Sie Acronis Cloud aus und klicken Sie dann auf **OK**.

   Sollten Sie bisher noch nicht angemeldet sein, dann geben Sie die E-Mail-Adresse und das Kennwort Ihres Acronis Kontos ein und klicken Sie dann auf **Anmelden**.

   Sollten Sie noch kein Acronis Konto haben, dann klicken Sie auf **Konto erstellen**, geben Sie Ihre E-Mail-Adresse und ein Kennwort ein – und klicken Sie dann auf die Schaltfläche **Konto erstellen**. Details finden Sie im Abschnitt 'Ein Acronis Konto erstellen'.
5. [Optionaler Schritt] Konfigurieren Sie die 'Erweiterten Einstellungen'. Sie können:

- Daten ausschließen, die mit den Diensten anderer Anbieter geschützt werden (sofern verwendet). Klicken Sie auf **Backup optimieren** und spezifizieren Sie die auszuschließenden Daten. Weitere Details finden Sie im Abschnitt 'Elemente vom Backup ausschließen'.
- Dateien und Ordner manuell unter **Einstellungen** –> **Ausschlusskriterien** ausschließen. Weitere Details finden Sie im Abschnitt 'Elemente vom Backup ausschließen'.
- Die Backup-Planung unter **Einstellungen** –> **Planung** konfigurieren. Weitere Informationen finden Sie im Abschnitt 'Planung'.
- Definieren Sie die Backup-Aufbewahrungsregeln unter **Einstellungen** –> **Bereinigung**. Weitere Informationen finden Sie im Abschnitt 'Backups, Backup-Versionen und Replikate bereinigen'.
- Ihr Backup per Kennwort und Verschlüsselung unter **Einstellungen** –> **Verschlüsselung** schützen. Weitere Details finden Sie im Abschnitt 'Backup-Verschlüsselung'.
- Wählen Sie das von Ihnen bevorzugte Datacenter und konfigurieren Sie die Upload-Geschwindigkeit (unter **Einstellungen** –> **Netzwerk**). Weitere Details finden Sie im Abschnitt 'Netzwerkeinstellungen für Backups'.
- Sie können die Backup-Versuche unter **Einstellungen** —> **Fehlerbehandlung** konfigurieren.

6. Wenn Sie alle Einstellungen konfiguriert haben und bereit zum Starten eines Backups sind, dann klicken Sie auf **Backup**.

**Hinweis**
Das erste Online Backup benötigt zur Fertigstellung möglicherweise eine längere Zeit. Zukünftige Backup-Prozesse werden voraussichtlich schneller ablaufen, da nur Änderungen an den Dateien gesichert werden.

Um Ihren Mac aus einem Acronis Cyber Protect Home Office Backup wiederherstellen zu können, benötigen Sie ein Acronis Boot-Medium. Sollten Sie noch keines haben, dann erstellen Sie es. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.

# Notarized Backup

Acronis Cyber Protect Home Office kann mithilfe der Blockchain-Technologie Ihre Dateien vor unbefugten Veränderungen schützen. Sie können damit überprüfen, dass es sich bei einer wiederhergestellten Datei auch wirklich exakt um diejenige Datei handelt, die Sie ursprünglich per Backup gesichert hatten. Wir empfehlen diese Art von Backup insbesondere zum Schutz rechtlich wichtiger Dokumente/Dateien. Sie können damit aber natürlich auch alle anderen Dateien schützen, deren Authentizität Sie überprüfen wollen. Genauere Informationen dazu finden Sie im Abschnitt 'Blockchain-Technologie verwenden'.

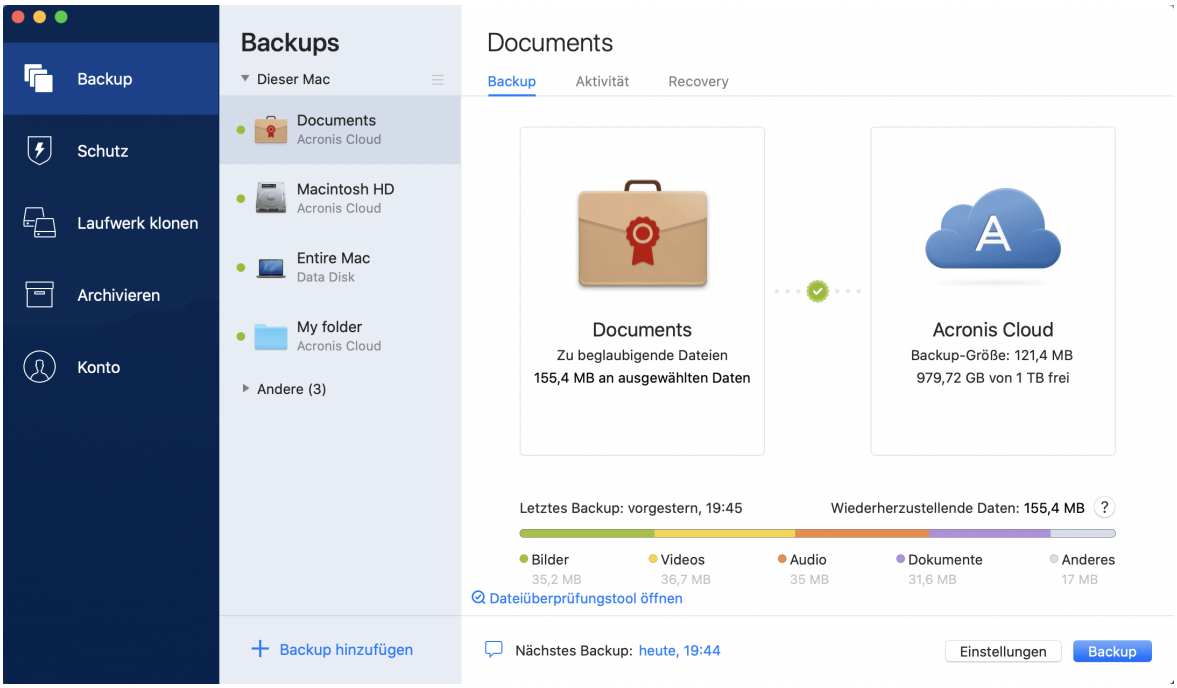
***So können Sie ein 'Notarized Backup' (Beglaubigtes Backup) Ihrer Dateien und Ordnern erstellen***

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Gehen Sie folgendermaßen vor:

- Überspringen Sie diesen Schritt, falls dies Ihr erstes Backup ist.
- Sollten Sie bereits ein Backup haben und stattdessen ein neues erstellen wollen, dann klicken Sie im unteren Bereich der Backup-Liste auf **Backup hinzufügen**.

**Hinweis**
Klicken Sie zum Löschen eines Backups mit der rechten Maustaste auf dieses und wählen Sie anschließend den Befehl **Löschen**. Das Backup wird daraufhin aus der Liste entfernt und die entsprechenden Backup-Dateien werden aus dem Backup Storage gelöscht.

3. Klicken Sie auf das Symbol für 'Backup-Quelle', dann auf **Zu beglaubigende Dateien** und bestimmen Sie anschließend, welche Dateien/Ordner Sie sichern wollen.




4. Klicken Sie auf das Symbol für das Backup-Ziel, bestimmen Sie den Speicherort für die Backup-Datei und klicken Sie dann auf **OK**. Sollte der Speicherort nicht aufgeführt sein, können Sie auf **Durchsuchen** klicken, um den Speicherort über den Verzeichnisbaum des Systems auszuwählen.

   Wenn Sie ein NAS-Gerät haben, wird dieses automatisch erkennt und zusammen mit den anderen Speicherorten in der Liste angezeigt.
5. [Optionaler Schritt] Konfigurieren Sie die 'Erweiterten Einstellungen'. Sie können:
   - Dateien und Ordner manuell unter **Einstellungen** –> **Ausschlusskriterien** ausschließen. Weitere Details finden Sie im Abschnitt 'Elemente vom Backup ausschließen'.

     Wenn Sie Dateien mit einer digitalen Signatur vom Backup ausschließen wollen, aktivieren Sie das Kontrollkästchen **Digital signierte Dateien nicht beglaubigen**. Weitere Details finden Sie im Abschnitt 'Elemente vom Backup ausschließen'.
   - Die Backup-Planung unter **Einstellungen** –> **Planung** konfigurieren. Weitere Informationen finden Sie im Abschnitt 'Planung'.

- Ihr Backup per Kennwort und Verschlüsselung unter **Einstellungen** –> **Verschlüsselung** schützen. Weitere Details finden Sie im Abschnitt 'Backup-Verschlüsselung'.
- Wählen Sie das von Ihnen bevorzugte Datacenter und konfigurieren Sie die Upload-Geschwindigkeit (unter **Einstellungen** –> **Netzwerk**). Weitere Details finden Sie im Abschnitt 'Netzwerkeinstellungen für Backups'.

6. Wenn Sie alle Einstellungen konfiguriert haben und bereit zum Starten eines Backups sind, dann klicken Sie auf **Backup**.

## Blockchain-Technologie verwenden

Acronis Cyber Protect Home Office verwendet die Blockchain-Technologie, um für Ihre per Backup gespeicherten Dateien mit einer zusätzlichen, modernsten Sicherheitsebene zu schützen. Diese Technologie gewährleistet, dass Ihre Dateien von keiner betrügerischen Software (unbemerkt) geändert werden. Denn wenn Sie eine Datei wiederherstellen wollen, können Sie überprüfen, dass es sich wirklich exakt um die Datei handelt, die Sie per Backup gesichert hatten.

### Was ist eine Blockchain?

Eine Blockchain (wörtlich etwa 'Datenblock-Kette') ist eine bestimmte Datenbank, in der Informationen über Transaktion und deren Reihenfolge gespeichert werden. Eine Transaktion entspricht dabei einem Ereignis. Das können beispielsweise Geldüberweisungen oder auch andere Aktionen mit Vermögenswerten (aller Art) sein. Diese Transaktionen werden in Blöcke zusammengefasst, die nacheinander in Form einer Blockchain (Datenblock-Kette) in die Datenbank geschrieben werden. Jede Transaktion und jeder Block hat dabei eine eigene, eindeutige Identifikationsnummer. Wichtig dabei ist, dass jeder Block zudem auch Informationen über alle vorherigen Blöcke in der Kette speichert. Sobald die Information über eine Transaktion in die Datenbank geschrieben wurde, kann diese von niemanden mehr geändert werden. Und auch die Transkationssequenz ist unveränderbar. Jeder Versuch, eine bestimmte Information in der Datenbank zu ändern, kann von jedem Benutzer der Datenbank leicht erkannt werden, weil in den nachfolgenden Blöcken die Informationen über die falsche Transaktion oder falschen Blöcke fehlen. Diese Technologie gewährleistet, dass in der Datenbank gespeicherte Daten gültig sind, zu einer bestimmten Person gehören und von niemanden geändert wurden. Weitere Informationen über die Blockchain-Technologie finden Sie unter der Adresse 'https://de.wikipedia.org/wiki/Blockchain'.

### So verwendet Acronis Cyber Protect Home Office die Blockchain-Technologie

Acronis Cyber Protect Home Office verwendet die Acronis Notary-Technologie, um Ihre Dateien vor unbefugten Veränderungen zu schützen. Dabei handelt es sich um eine universelle Lösung, um beliebige Datenobjekte/Datenströme mit digitalen Zeitstempeln und Fingerabdrücken zu versehen und zu vergleichen. Da es unpraktisch wäre, große Datenmengen in einer Blockchain-Datenbank zu speichern, sendet Acronis Cyber Protect Home Office nur die Hash-Werte von Dateien zum Acronis Notary Service.

Ein Hash-Wert (auch Hash-Code oder kurz einfach Hash) ist eine eindeutige Nummer mit festgelegter Größe, die von einer entsprechenden Hash-Funktion errechnet wird. Dieser Zahlencode

ist eine mathematische Definition für einen zufälligen Satz von Daten (beispielsweise von einer Backup-Datei). Jede Veränderung der Backup-Datei resultiert auch in einen abweichenden Hash-Wert. Wenn Sie also überprüfen wollen, ob eine Datei geändert wurde, müssen Sie nur ihre Hash-Werte vergleichen – und je einen Wert für den ursprünglichen Zustand der Datei und einen Wert für den aktuellen Zustand. Stimmen die Werte überein, so ist dies ein Beweis dafür, dass die Datei nicht verändert wurde.

Wenn Acronis Notary die Hash-Werte Ihrer Dateien empfängt, berechnet er einen neuen, einzelnen Hash-Wert und sendet diesen an die Blockchain-Datenbank von Ethereum. Ausführlichere Informationen (in Englisch) über Ethereum finden Sie unter der Adresse 'https://www.ethereum.org/'.

Sobald sich dieser Hash-Wert in der Datenbank befindet, werden die zur Berechnung des Hash-Codes verwendeten Dateien von Acronis Notary beglaubigt. Sie können die Authentizität eine Datei jederzeit leicht mit der im Abschnitt 'Die Authentizität von Dateien überprüfen' beschriebenen Prozedur überprüfen. Jede beglaubigte Datei hat ein Beglaubigungszertifikat (Notarization Certificate), welches der dokumentarischer Beleg dafür ist, dass diese Datei per Blockchain-Technologie geschützt wird. Ein solches Zertifikat enthält neben allgemeinen Informationen über die Datei außerdem technische Details, mit denen Sie die Dateiauthentizität manuell überprüfen können. Weitere Informationen finden Sie im Abschnitt 'Die Authentizität einer Datei manuell überprüfen'.

## Die Authentizität von Dateien überprüfen

Acronis Cyber Protect Home Office kann mithilfe der Blockchain-Technologie Ihre per Backup gesicherten Dateien vor unbefugten Veränderungen schützen. Sie können damit überprüfen, dass es sich bei einer wiederhergestellten Datei auch wirklich exakt um diejenige Datei handelt, die Sie ursprünglich per Backup gesichert hatten.

***So können Sie die Authentizität einer Datei in Acronis Cyber Protect Home Office überprüfen***

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Klicken Sie in der Seitenleiste auf **Backup**.
3. Wählen Sie in der Backup-Liste dasjenige 'Notarized Backup' aus, welches die zu überprüfende Datei enthält.
4. Öffnen Sie im rechten Fensterbereich die Registerkarte **Recovery**.
5. Suchen Sie die erforderliche Datei, klicken Sie auf das Pfeil-Symbol – und wählen Sie anschließend einen der nachfolgenden Befehle:
   - **Zertifikat anzeigen** – Das Zertifikat, welches ausführliche Informationen zur Dateisicherheit enthält, wird in Ihrem Webbrowser geöffnet.
   - **Überprüfen** – Acronis Cyber Protect Home Office wird die Authentizität der Datei verifizieren.

***So können Sie die Authentizität einer Datei im Dateiüberprüfungstool verifizieren:***

1. Öffnen Sie das Dateiüberprüfungstool mit einer der folgenden Methoden:
   - Öffnen Sie in einem Webbrowser die Adresse https://notary.acronis.com/verify.
   - Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office auf **Backup**, wählen Sie ein beglaubigtes Backup aus und klicken Sie dann im rechten Fensterbereich auf **Dateiüberprüfungstool öffnen**.
2. Suchen Sie im Finder die zu überprüfende Datei und ziehen Sie diese in das Webbrowser-Fenster.

***So können Sie die Authentizität einer Datei in Acronis Cloud überprüfen***

1. Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an.
2. Klicken Sie in der Seitenleiste auf **Backups**.
3. Wählen Sie in der Backup-Liste dasjenige 'Notarized Backup' aus, welches die zu überprüfende Datei enthält.
4. Wählen Sie die gewünschte Datei über deren Kontrollkästchen aus. Klicken Sie dann in der rechten Seitenleiste auf **Verifizieren**.

## Die Authentizität einer Datei manuell überprüfen

Die einfachste Möglichkeit, die Authentizität einer Datei zu verifizieren, besteht in der Verwendung des Befehls **Überprüfen**, der sowohl in Acronis Cyber Protect Home Office als auch in der Acronis Cloud verfügbar ist. Ausführliche Informationen dazu finden Sie im Abschnitt 'Die Authentizität von Dateien überprüfen'. Neben dieser einfachen Methode können Sie die Verifizierungsprozedur auch Schritt für Schritt selbst durchführen.

***So können Sie die Authentizität einer Datei manuell überprüfen***

**Schritt 1: Berechnen Sie den MD5-Hash-Wert der Datei**

1. Öffnen Sie die Applikation 'Terminal'.
2. Um beispielsweise den MD5-Hash-Wert (nachfolgend nur kurz MD5-Hash genannt) einer Datei namens 'picture.png' zu berechnen, geben Sie folgenden Befehl ein:

   ```
   $ md5 'picture.png'
   ```

   Beispiel für einen MD5-Hash: eea16ade1edf2750a46bb6bffb2e45a2
3. Überprüfen Sie, dass der berechnete MD5-Hash identisch ist mit einem eTag im Feld 'DATEN' in Ihrem Beglaubigungszertifikat (englisch auch als „Notarization Certificate“ bezeichnet). Informationen darüber, wie Sie ein Dateizertifikat abrufen können, finden Sie im Abschnitt 'Die Authentizität von Dateien überprüfen.

**Schritt 2. Überprüfen Sie, dass ein ROOT-Wert in der Blockchain gespeichert ist**

1. Öffnen Sie einen Blockchain-Explorer (beispielsweise https://etherscan.io/).
2. Geben Sie die TRANSAKTIONS-ID aus dem Zertifikat in das Suchfeld ein.

3. Überprüfen Sie, dass das Datenfeld in der Ereignisprotokoll-Registerkarte mit dem STAMMVERZEICHNIS (ROOT)-Wert in Ihrem Zertifikat übereinstimmt.

**Schritt 3. Überprüfen Sie, dass der Hash-Wert im Hash-Verzeichnisbaum enthalten ist**

1. Laden Sie das Befehlszeilenwerkzeug vom GitHub-Repository herunter: https://github.com/acronis/notary-verifyhash/releases.
2. Befolgen Sie die Anweisungen unter: https://github.com/acronis/notary-verifyhash.

# Mobilgeräte per Backup sichern

Falls Sie ein iOS- oder Android-Smartphone haben, können Sie Acronis Cyber Protect Home Office verwenden, um damit Ihre 'mobilen Daten' (wie Fotos, Videos, Kontakte und Kalendereinträge) zu sichern. Weitere Informationen finden Sie in der 'Dokumentation für Acronis Mobile'.

***So können Sie Mobilgerätedaten zu einem lokalen Storage auf Ihrem Computer sichern***

1. Folgende Voraussetzungen müssen erfüllt sein:
   - Acronis True Image (2017 oder höher) oder Acronis Cyber Protect Home Office ist auf Ihrem Computer installiert.
   - Auf Ihrem Mobilgerät ist die Acronis Mobile App installiert.
   - Ihr Computer und das Mobilgerät befinden sich im selben (W)LAN.
2. Auf Ihrem Computer:
   a. Starten Sie Acronis True Image (2017 oder höher) oder Acronis Cyber Protect Home Office.
   b. Klicken Sie in der Seitenleiste auf **Backup** und dann auf **Backup hinzufügen**.
   c. Klicken Sie auf den Bereich **Backup-Quelle** und wählen Sie **Mobilgerät**.
   Es wird ein QR-Code angezeigt. Schließen Sie dieses Fenster nicht, weil es gleich benötigt wird.
3. Auf Ihrem Mobilgerät:
   a. Acronis Mobile starten.
   b. Tippen Sie auf ein Plus-Symbol, um ein Backup zu erstellen. Beachten Sie, dass dieser Schritt nicht erscheint, wenn Sie Ihr Mobilgerät das erste Mal per Backup sichern.
   c. Wählen Sie einen Computer als Backup-Ziel.
   d. Tippen Sie auf **QR-Code scannen**, erfassen Sie den QR-Code auf dem Computer-Bildschirm mit Ihrer Kamera – und warten Sie dann, bis das Mobilgerät mit dem Computer verbunden ist.
   e. Wählen Sie die Datenkategorien aus, die Sie sichern wollen – oder tippen Sie auf **Bestätigen**, wenn Sie alle Kategorien sichern wollen.
   f. Erlauben Sie, dass Acronis Mobile auf Ihre persönlichen Daten zugreifen darf.
   g. [Optionaler Schritt] Geben Sie ein Kennwort ein, um das Backup per Verschlüsselung zu schützen. Anderenfalls können Sie auf **Verschlüsselung überspringen** tippen.
   h. Tippen Sie auf **Backup starten**.

Wenn das Backup gestartet ist, können Sie dessen Verlauf in beiden Applikationen (auf dem Computer oder Mobilgerät) verfolgen. Fehler und Warnmeldungen werden jedoch nur in der Mobile App angezeigt.

Sie können Acronis True Image oder Acronis Cyber Protect Home Office auf Ihrem Computer sowie die Acronis Mobile App nun schließen. Das Backup wird automatisch im Hintergrund fortgesetzt.

Nach Abschluss des Backups sind Ihre Daten zu Ihrem Computer übertragen worden. Wenn Sie möchten, dass Änderungen an den Daten (beispielsweise neue Fotos) automatisch gesichert werden sollen, aktivieren Sie die Einstellung **Kontinuierliches Backup**. Falls diese Einstellung ausgeschaltet ist, werden neue Daten nur dann gesichert, wenn Sie manuell auf **Backup** tippen.

Die Verbindung zwischen Ihrem Computer und dem Mobilgerät kann aufgrund eines Fehlers unterbrochen werden. Wählen Sie, um die Verbindung wiederherzustellen, das Mobilgeräte-Backup in der Backup-Liste von Acronis Cyber Protect Home Office aus, klicken Sie auf **Neu verbinden** und scannen Sie anschließend den QR-Code mit Ihrem Mobilgerät. Danach wird das Backup wieder normal mit den gleichen Einstellungen fortgesetzt.

# Acronis Mobile

**Hinweis**
Acronis Cloud ist möglicherweise in Ihrer Region nicht verfügbar. Für weitere Informationen klicken Sie hier: https://kb.acronis.com/content/4541

Mit Acronis Mobile können Sie die Daten Ihres Gerätes in die Acronis Cloud und/oder zu einem lokalen Storage auf Ihrem Computer sichern – um diese von dort (bei Datenverlust oder Datenbeschädigung) wiederherstellen zu können. Beachten Sie, dass Sie zur Backup-Erstellung in den Cloud Storage ein Acronis Cloud-Abonnement benötigen.

## Welche Geräte werden von der Mobile App unterstützt?

Sie können Acronis Mobile auf jedem Mobilgerät installieren, welches mit einem der folgenden Betriebssysteme läuft:

- iOS 12.0 und höher (iPhone, iPad, iPod)
- Android 7.0 und neuer (nur Smartphones)

## Kernfunktionen

Mit Acronis Mobile können Sie Folgendes tun:

- Ihre persönliche Daten sichern, einschließlich:
  - Fotos
  - Videos
  - Kontakte

    - Kalender
    - Nachrichten (nur bei Android-Geräten)
    - Erinnerungen (nur bei iOS-basierte Geräte)
- Wählen Sie einen der folgenden Speicherorte als Backup-Ziel aus:
    - Acronis Cloud
    - Einen lokalen Speicherort auf Ihrem Computer oder Mac
- Backup-Verschlüsselung mit AES-256-Algorithmus
- Automatisches Backup von neuen und veränderten Daten
- Mit jedem Ihrer Mobilgeräte auf die Cloud Backups zugreifen und Daten aus diesen Backups wiederherstellen

### Wo finde ich diese Apps?

Weitere Informationen über Acronis Mobile sowie die Möglichkeit zum Download/zur Installation finden Sie im Apple App Store oder Google Play Store.

- Acronis Mobile für iOS-Geräte: https://go.acronis.com/atimobile/download/iOS
- Acronis Mobile für Android-Geräte: https://go.acronis.com/atimobile/download/Android

## Lokaler Zielort für Backups von Mobilgeräten

Wenn Sie die Daten Ihres Mobilgerätes zu einem Computer sichern, speichert Acronis Cyber Protect Home Office die entsprechenden Backups im folgenden Standardordner: */Library/Application Support/Acronis Mobile Backup Data/acronis-local-data/*. Wenn Sie den Standardordner ändern, wird der Ordner *acronis-local-data* zu dem von Ihnen ausgewählten Speicherort als neuer Unterordner verschoben. Alle neu erstellten Mobile Backups werden dann zu dem neuen Speicherort erstellt.

**Hinweis**
Alle Mobile Backups werden immer in demselben Ordner gespeichert und können nicht getrennt werden.

***So können Sie den lokalen Zielort für die Mobilgeräte-Backups ändern***

1. Klicken Sie im Bereich **Backup** mit der rechten Maustaste auf ein Mobilgeräte-Backup und klicken Sie dann auf **Verschieben**.
2. Klicken Sie auf **Speicherort auswählen** und bestimmen Sie dann das neue Ziel für die Backups. Beachten Sie, dass Sie nur einen Speicherort (Ordner) auswählen können, der auf einem Ihrer internen Festplattenlaufwerke liegt.

Klicken Sie auf **Auf Standard zurücksetzen**, um den neuen Speicherort wieder zurück auf den ursprünglichen zu ändern.

# Microsoft 365-Daten per Backup sichern

## Warum sollten Sie Microsoft 365-Daten per Backup sichern?

Microsoft 365 ist zwar ein Set von Cloud-Diensten, ein regelmäßiges Backup bietet aber eine zusätzliche Schutzebene gegen Anwenderfehler und bösartige Angriffe. Acronis Cyber Protect Home Office kann Ihre Microsoft Outlook-Postfächer und Microsoft OneDrive-Daten schützen, indem es diese per Backup in die zuverlässige Acronis Cloud sichert. Außerdem können Sie nach dem Upload in die Acronis Cloud jederzeit und mit jedem internetfähigen Gerät auf all Ihre gesicherten Inhalte zugreifen (sofern das Gerät unterstützt und von Ihnen dazu berechtigt wird). Sie können gelöschte Elemente auch dann noch aus einem Backup wiederherstellen, wenn die offizielle Microsoft 365-Aufbewahrungsdauer abgelaufen ist.

## Microsoft 365-Daten per Backup sichern

**Diese Daten in Ihrem Outlook-Postfach können Sie sichern:**

- Alle Ordner
- E-Mail-Nachrichten
- Anhänge

**Hinweis**
Sie können keine freigegebenen Postfächer oder Gruppenpostfächer sichern.

**Diese Daten in Ihrem OneDrive können Sie sichern:**

- Alle Dateien und Ordner

**So können Sie Ihre Microsoft 365-Daten sichern:**

1. Öffnen Sie das Online Dashboard durch eine der folgenden Aktionen:
   - Folgen Sie diesem Link: https://cloud.acronis.com.
   - Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office nacheinander auf **Backup**, **Backup hinzufügen**, dann in den Bereich **Backup-Quelle** und wählen Sie anschließend auf **Cloud Service**.
2. Melden Sie sich an Ihrem Acronis Konto an.
3. Klicken Sie in der Seitenleiste erst auf **Ressourcen**, dann auf **Hinzufügen** und anschließend auf **Microsoft 365**.
4. Melden Sie sich bei Aufforderung an Ihrem Microsoft-Konto an.
5. Wählen Sie im Bereich **Backup-Quelle** die Elemente, die per Backup gesichert werden sollen:
   - Komplettes Konto
   - Outlook

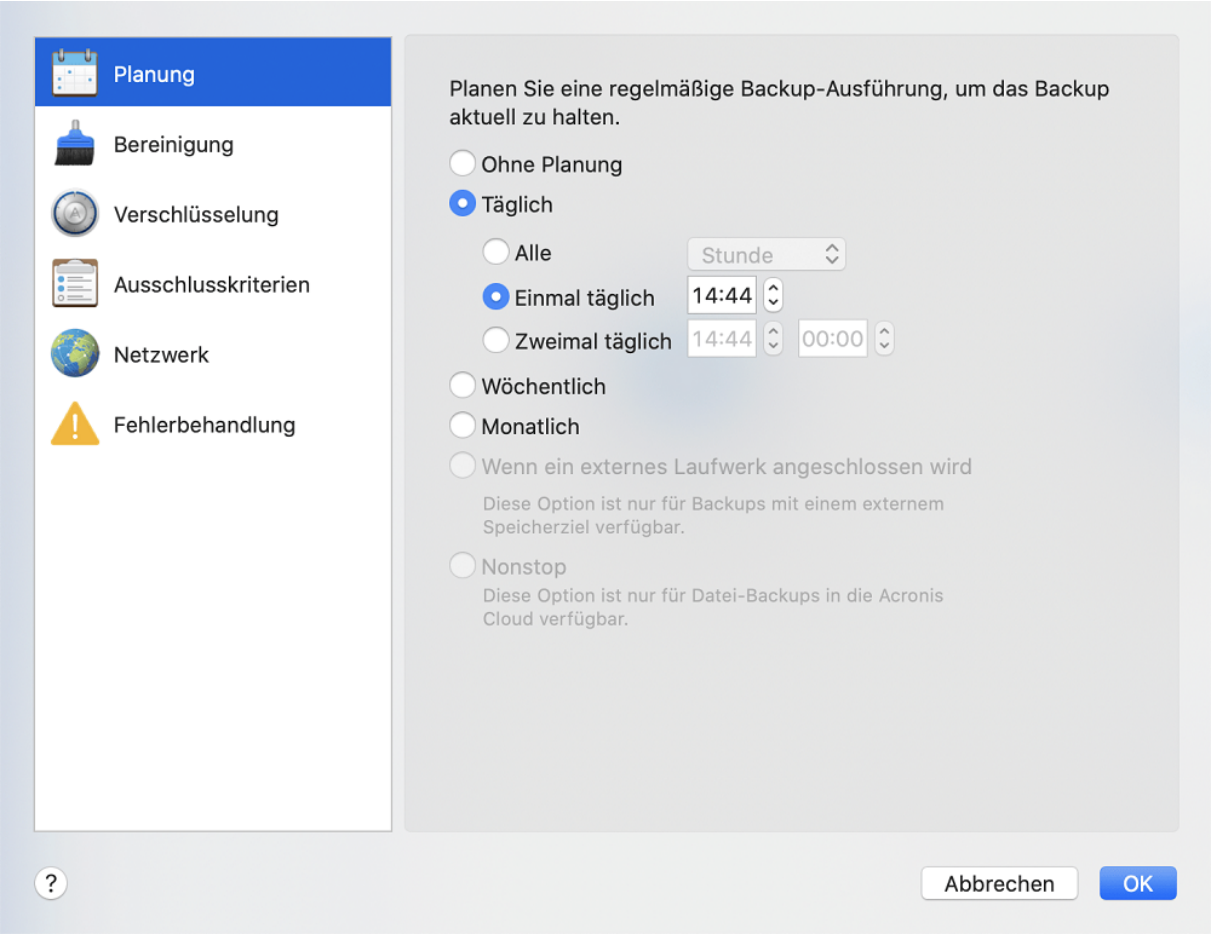
- OneDrive

6. Klicken Sie auf **Fertig**.
7. Im Fensterbereich **Bereinigung** können Sie Bereinigungsregeln für das Backup konfigurieren. Sie können das Backup außerdem verschlüsseln und mit einem Kennwortschutz versehen. Klicken Sie auf **Anwenden**, wenn Sie fertig sind.
8. Klicken Sie zum Starten des Backups auf **Jetzt ausführen**.

# Planung

**Hinweis**
Bestimmte Programmfunktionen sind in der von Ihnen verwendeten Edition möglicherweise nicht verfügbar.

Damit Ihre Backups auch wirklich hilfreich sind, sollten diese so aktuell wie möglich sein. Planen Sie Ihre Backups, um diese regelmäßig auszuführen. Standardmäßig wird Ihr Mac täglich gesichert.




***So können Sie ein Backup planen***

1. Klicken Sie auf **Einstellungen**, wählen Sie die Backup-Frequenz und spezifizieren Sie den Startzeitpunkt.

- **Ohne Planung**
  Durch diese Option wird die Planung ausgeschaltet.
- **Täglich**
  Das Backup startet ein- oder zweimal täglich zur spezifizierten Zeit oder mit einem von Ihnen festgelegten Zeitintervall.
- **Wöchentlich**
  Das Backup startet jede Woche an den ausgewählten Tagen und an dem von Ihnen spezifizierten Zeitpunkt.
- **Monatlich**
  Das Backup startet jeden Monat an den ausgewählten Daten und zum von Ihnen spezifizierten Zeitpunkt.
- **Wenn ein externes Laufwerk angeschlossen wird** (nur für Backups mit einem externen Speicherziel verfügbar)
  Wenn Sie einen Task planen, bei dem das Backup auf einen USB-Stick oder eine externe Festplatte erfolgen soll, wird das Backup jedes Mal automatisch gestartet, wenn dasselbe externe Gerät angeschlossen wird. Aktivieren Sie das Kontrollkästchen **Einmal täglich**, wenn das Backup zu dem Gerät nur einmal am Tag durchgeführt werden soll.
- **Nonstop** (nur für Cloud Backups auf Dateiebene verfügbar)
  Das anfängliche Voll-Backup enthält alle Daten, die ausgewählt wurden, um geschützt zu werden. Acronis Cyber Protect Home Office wird die zu schützenden Dateien dann kontinuierlich überwachen (inkl. Dateien, die in Anwendungen geöffnet sind). Sobald eine Änderung an den Dateien erkannt wird, werden die entsprechenden Daten gesichert. Das kürzeste Intervall zwischen zwei inkrementellen Backup-Aktionen beträgt fünf Minuten. Damit können Sie Ihre Daten zu einem bestimmten Zeitpunkt hin (in der Vergangenheit) wiederherzustellen bzw. auf diesen zurückzusetzen.

2. Klicken Sie auf **OK**, nachdem Sie alle Einstellungen konfiguriert haben.

Sollte Ihr Backup beim Erreichen des geplanten Zeitpunkts ausgeschaltet sein oder sich im Ruhezustand befinden, dann wird das Backup ausgeführt, wenn der Mac das nächste Mal startet oder aufgeweckt wird. Sie können den Power Nap-Modus Ihres Macs verwenden, um Ausfälle bei der Sicherung Ihrer Daten zu vermeiden.

## So können Sie den Mac Power Nap-Modus verwenden

- Aktivieren Sie in den Systemeinstellungen Ihres Mac die Power Nap-Option unter **Energie sparen** –> **Netzteil**.
- Klicken Sie im Menü von Acronis Cyber Protect Home Office auf **Einstellungen** -> **Allgemein** und aktivieren Sie dann das Kontrollkästchen **Backup, wenn Ihr Mac im Power Nap-Modus ist**. Klicken Sie auf **OK**.

Wenn diese Einstellung aktiviert ist, sich Ihr Mac im Ruhezustand befindet und dann der in der Backup-Planung eingestellte Backup-Zeitpunkt eintritt, wird das Backup beim nächsten Power Nap

ausgeführt. Beachten Sie, dass die Backup-Erstellung während eines Power Naps nur dann funktioniert, wenn Ihr Computer an das Stromnetz angeschlossen ist.

# Backup-Verschlüsselung

Um die gesicherten Daten gegen unberechtigte Zugriffe zu schützen, können Sie das Backup mit dem AES-Algorithmus (Advanced Encryption Standard) verschlüsseln lassen, wobei eine Verschlüsselungstiefe von 256 Bit verwendet wird.

**Hinweis**
Die Option zur Verschlüsselung eines Backups kann für bereits vorhandene Backups nicht mehr geändert werden.

***So können Sie ein Backup verschlüsseln***

1. Klicken Sie beim Konfigurieren eines Backups auf das Symbol für **Einstellungen** und dann auf die Option **Verschlüsselung**.
2. Geben Sie das Kennwort für das Backup in das enstprechende Feld ein und klicken Sie dann auf **OK**.
   Wir empfehlen die Verwendung eines Kennworts, das aus mindestens acht Zeichen besteht und sowohl Buchstaben (am besten Groß- und Kleinbuchstaben) wie Zahlen enthält, damit es nicht leicht zu erraten ist.
   Ein Kennwort kann nicht wieder abgerufen werden. Sie sollten das zum Backup-Schutz spezifizierte Kennwort daher gut speichern bzw. erinnern.

# Backups, Backup-Versionen und Replikate bereinigen

Bei jeder Ausführung einer Backup-Aktion, egal ob manuell oder per Planung, erstellt Acronis Cyber Protect Home Office am jeweiligen Backup-Speicherort eine neue Backup-Version.

Wenn Sie nicht mehr benötigte Backup-Versionen löschen wollen, sollten Sie dies nur mit den von der Applikation dafür bereitgestellten Befehlen tun. Wenn Sie einzelne Backup-Versionen außerhalb von Acronis Cyber Protect Home Office löschen wollen (z.B. mit dem Windows Explorer), wird dies zu Fehlern führen, wenn Sie mit den Backups weitere Aktionen durchführen wollen.

Die Versionen folgender Backups können nicht manuell gelöscht werden:

- Backups, die auf CD, DVD oder BD gespeichert sind.
- Nonstop Backups
- Beglaubigte Backups (Notarized Backups)

***Aufbewahrungsregeln für Nonstop Backups***

Wenn Sie Dateien und Ordner in die Acronis Cloud sichern, können Sie Planungseinstellungen für eine kontinuierliche Sicherung festlegen. Weitere Informationen finden Sie im Abschnitt 'Planung'.

Da Acronis Cyber Protect Home Office die Backup-Daten kontinuierlich überwacht und gefundene Datenänderungen in die Acronis Cloud hochlädt, kann das Backup den verfügbaren Speicherplatz möglicherweise schnell verbrauchen. Um die Anzahl der Backup-Versionen und den Speicherplatzverbrauch in der Cloud niedrig zu halten, behält Acronis Cyber Protect Home Office nur folgende Backup-Versionen:

- Alle Versionen der letzten Stunde
- Die ersten Versionen einer jeden Stunde der letzten 24 Stunden
- Die erste Version eines jeden Tages der letzten Woche
- Die erste Version einer jeden Woche des letzten Monats
- Die erste Version eines jeden Monats

Alle anderen Versionen werden automatisch gelöscht. Die Aufbewahrungsregeln sind voreingestellt und können nicht geändert werden.

***Replikat-Aufbewahrungsregeln***

Bei jeder Ausführung einer Backup-Aktion, bei der die Replikationsoption aktiviert ist, erstellt Acronis Cyber Protect Home Office eine neue Backup-Version an einem lokalen Speicherort und eine Replikat-Version in der Cloud. Manchmal ist die Anzahl der Replikat-Versionen etwas geringer als die Anzahl der Backup-Versionen. Das erfolgt, um Ihre Internetnutzung zu optimieren. Dennoch können die Replikate ziemlich viel Speicherplatz einnehmen. Verwenden Sie die Replikat-Aufbewahrungsregeln, um Speicherplatz zu sparen:

1. Klicken Sie im Bereich **Backup** auf das gewünschte Backup und dann in der unteren rechten Ecke auf den Befehl **Einstellungen**.
2. Klicken Sie auf **Einstellungen** und wählen Sie **Replikation**.

Sie können nun die Anzahl der Replikat-Versionen begrenzen. Sie können nicht nur die Anzahl der Replikate limitieren, sondern auch deren Alter. Aktivieren Sie das Kontrollkästchen **Lösche Versionen älter als** und spezifizieren Sie dann, wie lange eine Version (maximal) gespeichert werden soll. Alle Versionen, die älter als die spezifizierte Zeitspanne sind, werden automatisch gelöscht.

***So können Sie ein komplettes Backup und dessen Replikat löschen***

Klicken Sie im Bereich **Backup** mit der rechten Maustaste auf das Backup, zu dem das zu löschende Replikat gehört, und wählen Sie dann den Befehl **Backup und Replikat löschen**.

Abhängig vom Backup-Typ löscht dieser Befehl das Backup vollständig von seinem Speicherort – oder er erlaubt Ihnen zu wählen, ob Sie die Backup-Dateien vollständig löschen oder nur den Backup-Namen aus Acronis Cyber Protect Home Office entfernen wollen. Beachten Sie, dass die Löschung nicht rückgängig gemacht werden kann, wenn Sie ein Backup komplett löschen. Wenn Sie nur den Namen des Backups aus Acronis Cyber Protect Home Office entfernen, verbleiben die dazugehörigen Backup-Dateien an ihrem aktuellen Speicherort. Sie können das vorhandene Backup auch zu einem späteren Zeitpunkt wieder zu Acronis Cyber Protect Home Office hinzufügen.

Wenn ein Backup-Speicherort nicht mehr verfügbar ist, können die Backup-Dateien dort nicht mehr gelöscht werden. Sie können jedoch den Namen dieses Backups aus Acronis Cyber Protect Home Office entfernen. Wenn Sie Backup-Dateien löschen wollen, die Sie lokal, aber nicht in Acronis Cyber Protect Home Office sehen, sollten Sie versuchen, das entsprechende vorhandene Backup zuerst zu Acronis Cyber Protect Home Office hinzuzufügen. Danach können Sie das Backup und dessen Dateien mithilfe von Acronis Cyber Protect Home Office vollständig löschen.

Wenn Sie ein Backup löschen, wird automatisch auch dessen Replikat gelöscht. Sie können eine lokale Backup nicht löschen und dabei trotzdem dessen Replikat bewahren. Umgekehrt können Sie jedoch das Replikat alleine löschen und das entsprechende lokale Backup behalten.

Wenn Sie ein Replikat löschen wollen, ohne das entsprechenden Backup zu entfernen, dann müssen Sie im Bereich **Backup** mit der rechten Maustaste auf das Backup klicken, zu dem das zu löschende Replikat gehört, und anschließend den Befehl **Nur Replikat löschen** auswählen.

***So können Sie die Bereinigungseinstellungen konfigurieren***

1. Klicken Sie im Bereich **Backup** auf das gewünschte Backup und dann in der unteren rechten Ecke auf den Befehl **Einstellungen**.
2. Wählen Sie die Registerkarte **Bereinigung** aus und konfigurieren Sie die Bereinigungseinstellungen.

Standardmäßig speichert Acronis Cyber Protect Home Office die 20 letzten (neuesten) Versionen. Wenn Sie die 21. Version erstellen, löscht Acronis Cyber Protect Home Office automatisch die älteste Version des betreffenden Backups. Sie können einen anderen Wert für die Anzahl der Backup-Versionen festlegen.

# Ein vorhandenes Backup der Liste hinzufügen

Sie verfügen vielleicht über Backups von Acronis Cyber Protect Home Office, die Sie mit einer früheren Produktversion erstellt haben oder von einem anderen Computer herüberkopiert haben.

Sollten Sie Backups haben, die nicht in der Liste angezeigt werden, so können Sie diese manuell hinzufügen.

***So können Sie Backups manuell hinzufügen:***

1. Zeigen Sie im Menü **Datei** auf den Befehl **Vorhandenes Backup hinzufügen**. Das Programm öffnet ein Fenster, in dem Sie auf Ihrem Computer nach Backups suchen können.

   Sie können auch Spotlight verwenden, um nach .tib- oder .tibx-Dateien zu suchen.
2. Wählen Sie eine Backup-Version (eine .tib- oder eine .tibx-Datei). Daraufhin wird das komplette Backup zur Liste hinzugefügt.

Sie können Daten aus allen Backups in der Liste wiederherstellen. Sie können außerdem Backups, die auf demselben Mac erstellt wurde, rekonfigurieren.

***So können Sie ein Backup rekonfigurieren***

1. Klicken Sie auf das Symbol für 'Backup-Quelle' und bestimmen Sie, was gesichert werden soll.
2. [Optionaler Schritt] Planen Sie Ihr Backup, um dieses regelmäßig auszuführen.
3. Klicken Sie auf **Backup jetzt**, wenn Sie das Backup direkt starten wollen.

**Hinweis**
Wenn Sie ein lokales Backup aus der Liste verbergen wollen, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf den Befehl **Aus der Liste verbergen**. Sie werden mit diesem Backup solange keine Aktionen durchführen können, bis Sie es manuell wieder in die Liste aufnehmen.

# Elemente vom Backup ausschließen

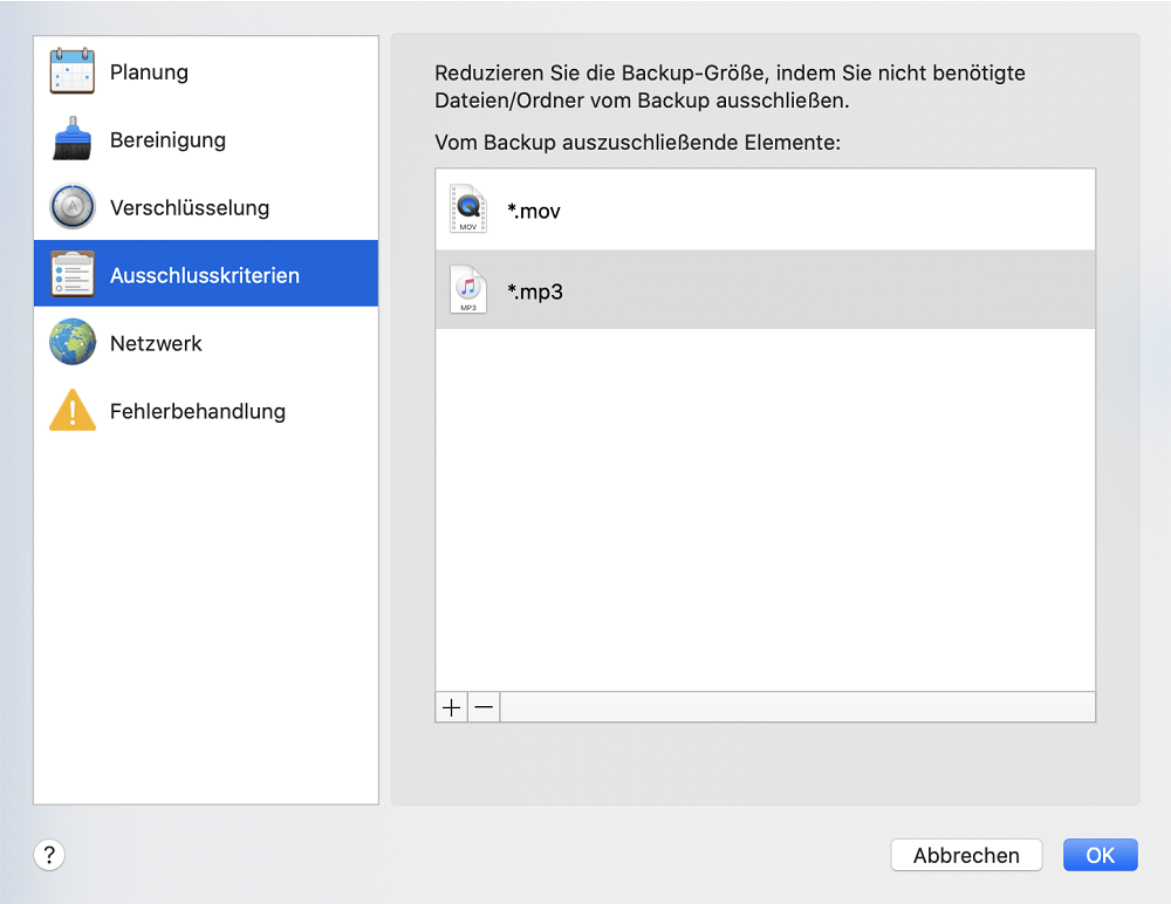
Sie können die Größe eines Backups schon vor dessen Start reduzieren, indem Sie solche Daten ausschließen, die nicht mitgesichert werden müssen.

Sie können Dateien und Ordner folgendermaßen ausschließen:

- **Manuell, von jedem Backup**
  Um ein Element ausschließen zu können, müssen Sie es genau spezifizieren oder eine Maske verwenden.
- **Automatisch, von einem Backup in die Acronis Cloud**
  Acronis Cyber Protect Home Office analysiert die verwendete Backup-Quelle und schlägt Ihnen zum Ausschließen lokale Daten vor, die aus den Cloud-Speichern von Drittanbietern heruntergeladen werden können.

## Elemente manuell ausschließen

1. Klicken Sie beim Konfigurieren eines Backups auf **Einstellungen** und dann auf den Befehl **Ausschlusskriterien**.




2. Klicken Sie auf das Plus-Symbol und dann auf eine der folgenden Optionen:
   - **Bestimmte Datei oder Ordner ausschließen**

     Finden Sie das auszuschließende Element, wählen Sie es aus und klicken Sie dann auf **Ausschließen**.
   - **Per Maske ausschließen**

     Geben Sie unter Verwendung von Platzhalterzeichen (* und ?) eine Ausschlussmaske ein und klicken Sie dann auf **Ausschließen**.

     Beispiele für Ausschlussmasken:
     - **.ext* – Alle Dateien mit der Erweiterung '.ext' werden ausgeschlossen.
     - *??name.ext* – Dateien mit der Erweiterung '.ext', deren Namen aus sechs Buchstaben bestehen (beginnend mit zwei beliebigen Zeichen (??) und mit *name* endend), werden ausgeschlossen.
3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Digital signierte Dateien nicht beglaubigen** (nur bei einem Notarized Backup verfügbar).

   Der Hauptzweck eines Notarized Backups ist der Schutz Ihrer persönlichen Dateien vor unbefugten Veränderungen. Es ist daher nicht unbedingt notwendig, Dateien, die bereits eine digitale Signatur haben (wie Betriebssystemdateien, Applikationsdateien), in einem solchen Backup mitzusichern. Sie können diese Dateien ausschließen, wenn Sie das entsprechende Kontrollkästchen aktivieren.
4. Klicken Sie auf **OK**.

## Anderweitig wiederherstellbare Daten von Online Backups ausschließen

Sie können mit Acronis Cyber Protect Home Office solche lokale Daten ausschließen, die über die Cloud-Dienste anderer Anbieter (wie Google Drive oder Dropbox) hochgeladen bzw. synchronisiert werden. Diese Daten sind bereits geschützt und können jederzeit leicht auf Ihren Computer heruntergeladen werden. Es ist daher nicht notwendig, diese zusätzlich in die Acronis Cloud hochzuladen. Sie können die Daten vom Backup ausschließen, um dessen Größe zu reduzieren und den Backup-Prozess zu beschleunigen.

Sie können Daten ausschließen, die durch folgende Dienstleister geschützt werden:

- iTunes
- Dropbox
- Microsoft OneDrive
- Google Drive
- BoxSync
- Yandex.Disk
- SugarSync

Acronis Cyber Protect Home Office schlägt Ihnen nur dann das Ausschließen solcher Daten vor, wenn folgende Kriterien zutreffen:

- Der Dienst des Drittanbieters ist zum Backup-Zeitpunkt aktiviert.
- Die im entsprechenden Ordner gespeicherte Datenmenge beträgt über 250 MB.

***So können Sie Elemente von einem Online Backup ausschließen***

1. Klicken Sie vor dem Start des Backup-Prozesses auf den Befehl **Backup optimieren** (unterhalb des Symbols für die Backup-Quelle).
2. Aktivieren Sie die Kontrollkästchen neben den Elementen, die Sie vom Backup ausschließen wollen – und klicken Sie dann auf **Fertig**.

# Verbindungseinstellungen

Wenn Sie sich mit einem Computer im Netzwerk oder einem NAS-Gerät verbinden, müssen Sie normalerweise Anmeldedaten spezifizieren, um auf den entsprechenden Netzwerk-Speicherort zugreifen zu können. Dies ist beispielsweise möglich, wenn Sie einen Backup-Ziel auswählen. Falls die Anmeldedaten des Netzwerk-Speicherortes geändert wurden, müssen Sie diese in den Backup-Einstellungen manuell korrigieren. Anderenfalls werden alle weiteren Backup-Aktionen fehlschlagen.

***So können Sie die Anmeldedaten für einen Netzwerk-Speicherort ändern***

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Wählen Sie im Bereich **Backup** dasjenige Backup aus, welches einen Netzwerk-Speicherort als Quelle oder Ziel verwendet.
3. Klicken Sie auf das Zahnradsymbol, um die Backup-Einstellungen zu öffnen.
4. Spezifizieren Sie im Bereich **Verbindung** die Anmeldedaten (Benutzername, Kennwort), um auf den Netzwerk-Speicherort zugreifen zu können.
5. [Optionaler Schritt] Klicken Sie auf **Verbindung testen**.
   Wenn die Verbindung aufgebaut wird, sind die Anmeldedaten korrekt.
6. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

# Netzwerkeinstellungen für Backups

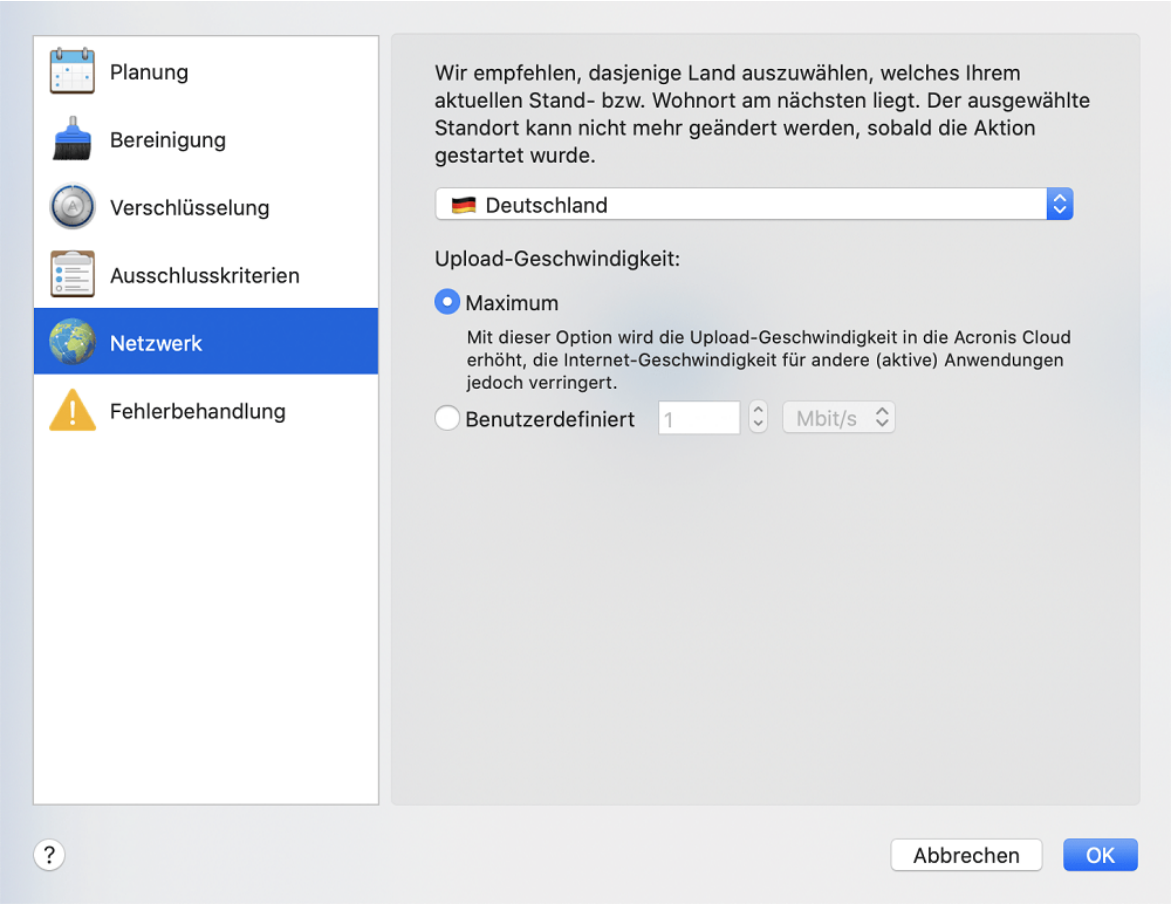
Wenn Sie bei der Erstellung eines Backups die Acronis Cloud Cloud als Ziel verwenden, werden Ihre Daten in eines der Acronis Datacenter hochgeladen, die jeweils in verschiedenen Ländern liegen. Beim Erstellen Ihres Acronis Kontos wird anfänglich dasjenige Datacenter für Sie festgelegt, welches Ihrem Standort am nächsten liegt. Anschließend werden Ihre Online Backups und synchronisierten Dateien standardmäßig in genau diesem Datacenter gespeichert.

Wir empfehlen, dass Sie dann ein anderes Datacenter für Ihre Backups manuell festlegen, wenn Sie sich in einem anderen Land befinden – oder das standardmäßig ausgewählte Datacenter doch nicht das nächstliegende ist (bezogen auf Ihren Stand- bzw. Wohnort). Dies kann die Datenrate beim Upload deutlich steigern.

**Hinweis**
Sie können das Datacenter für dort bereits vorliegende Backups nicht mehr ändern.

***So können Sie ein Datacenter auswählen***

1. Klicken Sie beim Konfigurieren eines Online Backups zuerst auf **Einstellungen** und dann auf **Netzwerk**.




2. Wählen Sie dasjenige Land aus, das am nächsten zu Ihrem aktuellen Stand- bzw. Wohnort liegt. Klicken Sie anschließend auf **OK**.

## Upload-Geschwindigkeit

Wenn Sie Daten in die Acronis Cloud sichern, können Sie festlegen, welche maximale Netzwerkverbindungsgeschwindigkeit Acronis Cyber Protect Home Office dabei verwenden soll. Legen Sie dazu diejenige Verbindungsgeschwindigkeit fest, die es Ihnen ermöglicht, das Internet und andere Netzwerkverbindungen weiter ohne störende Verlangsamung zu nutzen.

1. Gehen Sie in den Backup-Einstellungen zum Bereich **Netzwerk**.
2. Verwenden Sie eine der folgenden Optionen, um die Verbindungsgeschwindigkeit festzulegen:
   - **Maximum** – Die Datenübertragungsrate ist (auf Basis der Grenzen der vorhandenen Systemkonfiguration) maximal.
   - **Benutzerdefiniert** – Sie können für die Upload-Geschwindigkeit einen maximalen Wert festlegen.

# Backup-Aktivität und -Statistiken

In den Registerkarten **Aktivität** und **Backup** werden Ihnen weitere Informationen über ein Backup angezeigt – beispielsweise der Backup-Verlauf und die im Backup enthaltenen Dateitypen. Die Registerkarte **Aktivität** enthält eine Liste der Aktionen, die mit dem ausgewählten Backup seit

seiner Erstellung durchgeführt wurden. Zusätzlich werden Statusmeldungen und Statistiken zu den Aktionen angezeigt. Das kann praktisch, wenn Sie herausfinden wollen, was mit einem Backup im Hintergrundmodus passiert ist. Angezeigt werden Informationen wie die Anzahl und der Status von geplanten Backup-Aktionen, die Größe der gesicherten Daten usw.

Wenn Sie die erste Version eines Backups erstellen, wird Ihnen in der Registerkarte **Backup** eine grafische Darstellung über den Backup-Inhalt auf Basis der gesicherten Dateitypen angezeigt.

## Die Registerkarte 'Aktivität'

**Hinweis**
Für Nonstop-Backups und die Backups von Mobilgeräten gibt es keine Aktivitätsinformationen.

***So können Sie sich eine Backup-Aktivität anzeigen lassen***

1. Klicken Sie in der Seitenleiste auf **Backup**.
2. Wählen Sie in der Backup-Liste dasjenige Backup aus, dessen Verlauf Sie sich ansehen wollen.
3. Klicken Sie im rechten Fensterbereich auf **Aktivität**.

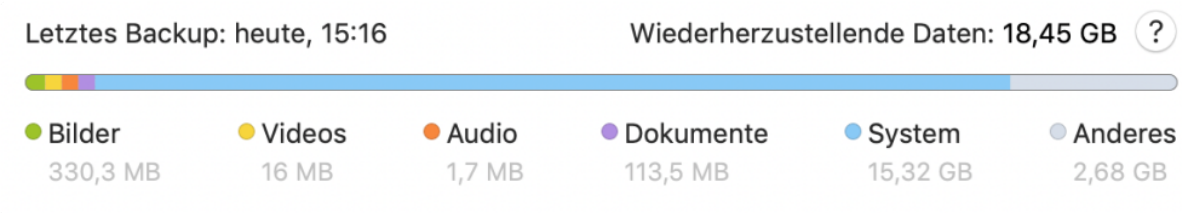

**Was Sie einsehen und analysieren können:**

- Backup-Aktionen und deren Statuszustände (erfolgreich, fehlgeschlagen, abgebrochen, unterbrochen usw.)
- Mit dem Backup durchgeführte Aktionen und deren Statuszustände.
- Fehlermeldungen
- Backup-Kommentare
- Details zu einer Backup-Aktion, einschließlich:
  - **Gesichert** – Größe der im Backup (mit Komprimierung) gespeicherten Daten.
  - **Geschwindigkeit** – Geschwindigkeit der Backup-Aktion.
  - **Dauer** – Zeitdauer, die zur Durchführung der Backup-Aktion benötigt wurde.
  - **Wiederherstellbar** – Anfängliche Größe der Daten (ohne Komprimierung).
  - **Methode** – Art der Backup-Aktion (vollständig, inkrementell).

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/de/content/60104.

## Die Registerkarte 'Backup'

Wenn ein Backup erstellt wird, werden Ihnen hier Statistiken über die Art der gesicherten Dateien angezeigt:




Zeigen Sie auf ein Farbsegment, um die Anzahl der Dateien und die Gesamtgröße für jede Datenkategorie einzusehen:

- Bilder
- Videodateien
- Audiodateien
- Dokumente
- Systemdateien
- Andere Dateitypen (inkl. versteckte Systemdateien)

**Wiederherzustellende Daten** – zeigt die Größe der ursprünglichen Daten an, die Sie für das Backup ausgewählt haben.

# Energieeinstellungen für Notebooks und Tablets

**Hinweis**
Diese Einstellung ist nur auf Computern mit Akkus (wie Notebooks, Tablets, Computer mit einer USV) verfügbar.

Wenn Sie ohne Ladegerät/Netzteil mit Ihrem Notebook oder Tablet arbeiten (weil keines verfügbar ist oder der Computer aufgrund eines Stromausfalls auf eine USV umgeschaltet wurde), kann es angebracht sein, die Akkuladung Ihres Gerätes zu schonen. Manchmal können länger dauernde Backups den Akku recht stark belasten.

***So können Sie Akkuladung einsparen***

- Klicken Sie im Menü von Acronis Cyber Protect Home Office auf **Einstellungen** -> **Energiesparmodus** und aktivieren Sie dann das Kontrollkästchen **Kein Backup, wenn der Akkustand niedriger ist als**. Klicken Sie anschließend auf **OK**.

Wenn diese Einstellung aktiviert ist und Sie ohne Ladegerät/Netzteil arbeiten (weil Sie dieses herausgezogen haben oder der Computer aufgrund eines Stromausfalls auf eine USV umgeschaltet wurde) und wenn dann die aktuelle Akkuladung den Wert erreicht, den Sie per Schieberegler

festgelegt haben, werden alle gerade laufenden Backups pausiert und in Planung befindliche Backups (vorerst) nicht mehr gestartet. Die pausierten Backups werden fortgesetzt, sobald das Ladegerät/Netzteil wieder angeschlossen wird bzw. die Stromversorgung wieder verfügbar ist. Geplante Backups, die aufgrund der Einstellung ausgesetzt wurden, werden ebenfalls gestartet.

Diese Einstellung blockt die Backup-Funktionalität aber nicht komplett. Denn Sie können ein Backup immer noch manuell starten.

Lokale Backups für Mobilgeräte sind von der Einstellung nicht betroffen. Ihre Mobilgerätedaten werden wie gewohnt zu einem lokalen Speicherort auf Ihrem Computer gesichert.

# WLAN-Verbindungen für Backups in die Acronis Cloud

Wenn Sie Ihre Daten in die Acronis Cloud sichern wollen, sorgen Sie sich möglicherweise um die Sicherheit Ihrer persönlichen Daten, falls die Übertragung über ein ungeschütztes (z.B. öffentliches) WLAN-Netzwerk erfolgen sollte. Um das Risiko zu vermeiden, dass Ihre persönlichen Daten gestohlen werden, empfehlen wir, dass Sie nur geschützte (nicht öffentliche) WLAN-Verbindungen für Backups verwenden.

***So können Sie Ihre Daten schützen***

- Klicken Sie im Menü von Acronis Cyber Protect Home Office zuerst auf **Einstellungen**, dann auf **WLAN-Verbindungen** und wählen Sie anschließend die Option **Backup nur bei ausgewählten WLAN-Verbindungen**. Aktivieren Sie in der Box **Gespeicherte Netzwerke** (hier werden früher verwendete WLAN-Verbindungen gespeichert) die Kontrollkästchen derjenigen WLAN-Verbindungen, die zur Sicherung Ihrer Daten verwendet werden dürfen.

Wenn die entsprechenden WLANs ausgewählt sind und Ihr Computer die Verbindung zu einem dieser Netzwerke verliert, werden alle aktuellen Backups pausiert und geplante Backups (vorerst) nicht gestartet. Die pausierten Backups werden wieder fortgesetzt, sobald der Computer wieder mit einem dieser sicheren Netzwerke verbunden ist. Geplante Backups, die aufgrund der Einstellung ausgesetzt wurden, werden ebenfalls gestartet.

Wenn Sie Ihre Daten über eine neue WLAN-Verbindung sichern wollen, können Sie dieses Netzwerk einfach auf Ihrem Computer speichern und dann in der Box **Gespeicherte Netzwerke** auswählen. Sie können dies jederzeit durchführen, wenn Sie eine neue Netzwerkverbindung benötigen.

Lokale Backups für Mobilgeräte sind von der Einstellung nicht betroffen. Ihre Mobilgerätedaten werden wie gewohnt zu einem lokalen Speicherort auf Ihrem Computer gesichert.

# Benachrichtigungen

## Benachrichtigungen in der macOS Mitteilungszentrale

Sie können die internen Benachrichtigungen von Acronis Cyber Protect Home Office zusätzlich (also als Duplikate) auch noch in der macOS Mitteilungszentrale (Notification Center) anzeigen lassen. Dadurch können Sie die Benachrichtigungen an dem von Ihnen bevorzugten Ort lesen, ohne die

Benutzeroberfläche von Acronis Cyber Protect Home Office öffnen zu müssen. Die Benachrichtigungen werden automatisch in der macOS Mitteilungszentrale angezeigt.

Wenn Sie produktinterne Benachrichtigungen in die Mitteilungszentrale duplizieren wollen, müssen Sie zuerst im Acronis Cyber Protect Home Office-Menü auf **Einstellungen** klicken und dann das Kontrollkästchen **Benachrichtigungen in der Mitteilungszentrale anzeigen** aktivieren.

## Benachrichtigungen im Acronis Tray Notification Center

Wenn Acronis Cyber Protect Home Office geöffnet ist, können Sie dort den Status einer jeden Aktion einsehen. Da einige Aktionen (wie Backups) jedoch eine längere Zeit dauern können, müssen Sie Acronis Cyber Protect Home Office nicht die ganze Zeit geöffnet halten, um über das Ergebnis der Aktion(en) informiert zu werden. Die Benachrichtigungen in der macOS Mitteilungszentrale bleiben solange vorhanden, bis Sie diese schließen. Sie können eine einmal geschlossene Benachrichtigung jedoch nicht wieder öffnen. Um diese Information zu sehen, müssen Sie Acronis Cyber Protect Home Office öffnen.

Das Tray Notification Center zeigt die neuesten Benachrichtigungen an einem Ort an, sodass Sie wichtige Statusmeldungen einsehen können, ohne Acronis Cyber Protect Home Office jedes Mal öffnen müssen, wenn Sie die Benachrichtigungen benötigen. Die folgenden Benachrichtigungen werden im Acronis Tray Notification Center angezeigt: persönliche Angebote, Informationen über die Ergebnisse von Backup-Aktionen und andere wichtige Benachrichtigungen von Acronis Cyber Protect Home Office. Das Tray Notification Center wird minimiert angezeigt und ist unter Acronis Cyber Protect Home Office in der Mac-Leiste verborgen.

## E-Mail-Benachrichtigungen über den Backup-Status

Wenn Sie nicht auf die Fertigstellung eines Backups warten wollen oder wenn Sie Ihre geplanten Backups grundsätzlich überwachen wollen, können Sie sich Backup-Statusberichte praktischerweise auch an Ihre E-Mail-Adresse senden lassen. Das ermöglicht Ihnen, auch dann umgehend über Backup-Probleme informiert zu sein, wenn Sie nicht direkt vor Ihrem Computer sitzen.

***So können Sie die E-Mail-Benachrichtigungen konfigurieren***

1. Klicken Sie im Acronis Cyber Protect Home Office-Menü auf **Einstellungen für E-Mail-Benachrichtigungen**.
   Die Seite **E-Mail-Benachrichtigungen** des Online Dashboards wird in Ihrem Webbrowser geöffnet.
2. Bestimmen Sie, welche Benachrichtigungstypen Sie erhalten wollen.
3. Geben Sie die E-Mail-Adresse ein, an welche die Benachrichtigungen gesendet werden sollen.
4. Geben Sie unter Verwendung der nachfolgenden Variablen eine Vorlage für die Nachrichten-Betreffzeile ein:
   - [Computer-Name]
   - [Aktionsstatus]
   - [Backup-Name]

Sie können beispielsweise Folgendes eingeben: *Backup-Bericht: [Backup-Name] - [Aktionsstatus] auf [Computer-Name]*

5. Klicken Sie auf **Speichern**.

# Unterstützung für Parallels Desktop

## Was ist Parallels Desktop?

Parallels Desktop ist eine Anwendung, die es ermöglicht, ein anderes Betriebssystem auf Ihrem Mac mithilfe einer besonderen virtuellen Umgebung auszuführen. Es wird normalerweise verwendet, um Windows auszuführen. Aber Sie können auch macOS, Linux, Google ChromeOS und andere Betriebssysteme ausführen. Weitere Details dazu können Sie erfahren, wenn Sie die Parallels-Website besuchen: https://www.parallels.com/de/products/desktop/.

## Wie handhabt Acronis Cyber Protect Home Office virtuelle Parallels Desktop-Maschinen?

Acronis Cyber Protect Home Office bietet eine vollständige Unterstützung für virtuelle Maschinen, die mit Parallels Desktop 16 (und höheren Versionen) erstellt wurden. Wenn Sie ein Backup Ihres Macs erstellen, werden auch die virtuellen Maschinen mitgesichert. Wenn Sie Ihren Mac wiederherstellen, werden die virtuellen Maschinen auf den Zustand zurückversetzt, in dem diese zum Zeitpunkt der Backup-Erstellung vorlagen. Nach einer Wiederherstellung sind all Ihre virtuellen Maschinen weiterhin konsistent und bootfähig.

## Wie funktioniert das?

Bei jeder Backup-Ausführung erstellt Acronis Cyber Protect Home Office sogenannte Snapshots aller virtuellen Parallels Desktop-Maschinen, die auf/in den zum Backup ausgewählten Laufwerken/Ordnern gespeichert sind. Diese Snapshots werden als spezielle (Recovery-)Zeitpunkte verwendet, wenn Sie Ihren Mac wiederherstellen. Nachdem die erstellten Snapshots in dem jeweiligen Backup gespeichert wurden, werden sie automatisch von Ihrem Mac gelöscht.

## Welche virtuellen Maschinen werden per Backup gesichert?

Acronis Cyber Protect Home Office sichert alle virtuellen Maschinen, die:

- auf den per Backup gesicherten Laufwerken gespeichert sind
- zur Parallels Desktop-Anwendung hinzugefügt wurden
- derzeit laufen, gestoppt oder angehalten (pausiert) sind

## Wie kann ich virtuelle Maschinen wiederherstellen?

Wenn Ihre virtuellen Maschinen (VMs) mit Parallels Desktop 16 (oder höher) erstellt wurden, werden alle wiederhergestellten VMs nach der Wiederherstellung direkt bootfähig sein. Wenn Sie eine ältere

Version von Parallels Desktop verwendet haben, sollten Sie das Skript 'recreate_pd_hdd.sh' ausführen, um die Bootfähigkeit Ihrer VMs wiederherzustellen.

In Acronis True Image (2017 oder höher) wird dieses Skript zusammen mit dem Produkt ausgeliefert und befindet sich im folgenden Verzeichnis: /Applications/Acronis True Image.app/Contents/MacOS/recreate_pd_hdd.sh. In Acronis Cyber Protect Home Office wird dieses Skript zusammen mit dem Produkt ausgeliefert und befindet sich im folgenden Verzeichnis: /Applications/Acronis Cyber Protect Home Office.app/Contents/MacOS/recreate_pd_hdd.sh. Sollten Sie noch eine ältere Produktversion verwenden, dann können Sie die Skriptdatei von dieser Adresse herunterladen: https://kb.acronis.com/system/files/content/2016/08/49198/recreate_pd_hdd.zip.

***So können Sie das Skript ausführen***

1. Entpacken Sie das Skript (die .zip-Datei).
2. Öffnen Sie die Applikation 'Terminal'.
3. Geben Sie den Befehl *bash "[script_path]" "[vm_path]"* ein. Dabei steht:
   - [script_path] für den Pfad zu der Skriptdatei.
   - [vm_path] für den Pfad zu dem Ordner, wo sich die wiederhergestellten Dateien der virtuellen Maschine befinden.

   Zum Beispiel:

   ```
   bash "/Applications/Acronis Cyber Protect Home Office.app/Contents/MacOS/recreate_pd_
   hdd.sh" "/Users/John/Downloads/My Windows Virtual Machine.pvm"
   ```

**Hinweis**
Wir empfehlen, die PD-Maschinen als neue VMs wiederherzustellen, statt die vorherigen zu überschreiben.

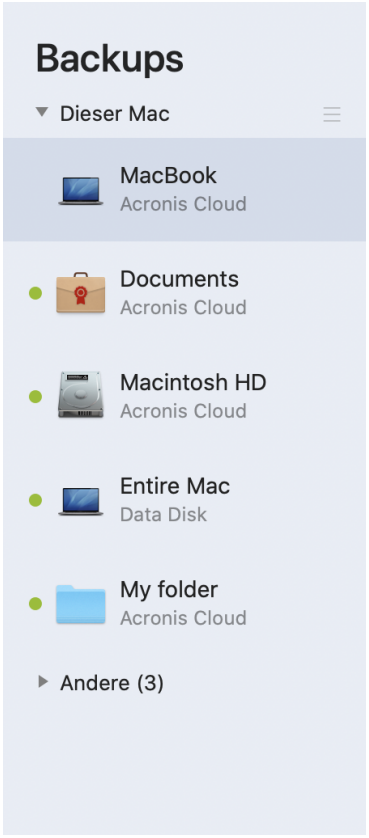
## Einschränkungen

Falls Sie virtuelle Parallels Desktop-Maschinen so konfiguriert haben, dass diese das Boot Camp-Volume verwenden, sollten Sie folgende Beschränkungen beachten:

- Wenn die virtuelle Maschine gerade läuft, wird ein Backup der Boot Camp-Partition in den meisten Fällen fehlschlagen.
- Wenn die virtuelle Maschine angehalten wurde, wird ein Backup der Boot Camp-Partition erfolgreich funktionieren, aber eine Wiederherstellung aus diesem Backup wird in den meisten Fällen fehlschlagen.
- Wenn die virtuelle Maschine angehalten wurde, wird eine Wiederherstellung zur Boot Camp-Partition fehlschlagen. Entfernen Sie stattdessen die Boot Camp-Partition und führen Sie die Wiederherstellung aus dem Backup dann zum 'nicht zugeordneten' Speicherplatz durch.

# Backup-Liste

Wenn Sie mit der Backup-Liste arbeiten, werden besondere Symbole (Icons) angezeigt. Die Symbole zeigen Ihnen einen Backup-Typ und den aktuellen Backup-Zustand an.




## Backup-Stadien

| Symbol | Beschreibung |
|---|---|
| ● | Das Backup wurde erfolgreich abgeschlossen. |
| ● | Das Backup befindet sich in der Warteschlange. |
| ● (blinkend) | Das Backup wird ausgeführt. |
| ○ | Das Backup wurde vom Benutzer pausiert. |
| ● | Das letzte Backup ist fehlgeschlagen. |
| ● | Das Backup wurde mit Warnungen abgeschlossen. |

## Backups in der Liste sortieren

Die Backups werden standardmäßig nach Ihrem Erstellungsdatum sortiert, beginnend vom neuesten bis runter zum ältesten. Sie können die Reihenfolge ändern, indem Sie den entsprechenden Sortierungstyp im oberen Bereich der Backup-Liste auswählen. Sie haben folgende Optionen:

| Befehl | | Beschreibung |
|---|---|---|
| **Sortieren nach** | **Name** | Dieser Befehl sortiert alle Backups in alphabetischer Reihenfolge.<br>Wählen Sie **Z —> A**, um die Reihenfolge umzudrehen. |
| | **Erstellungsdatum** | Dieser Befehl sortiert alle Backups von den neuesten zu den ältesten.<br>Wählen Sie **Ältere zuerst**, um die Reihenfolge umzudrehen. |
| | **Aktualisierungszeitpunkt** | Dieser Befehl sortiert alle Backups nach dem Datum der letzten Version. Je neuer die letzte Backup-Version, desto höher wird das Backup in der Liste positioniert.<br>Wählen Sie **Ältere zuerst**, um die Reihenfolge umzudrehen. |
| | **Größe** | Dieser Befehl sortiert die Backups nach Größe, beginnend mit dem größten bis hin zum kleinsten.<br>Wählen Sie **Kleinste zuerst**, um die Reihenfolge umzudrehen. |
| | **Quelltyp** | Dieser Befehl sortiert alle Backups nach dem Quelltyp. |
| | **Zieltyp** | Dieser Befehl sortiert alle Backups nach dem Zieltyp. |

# Recovery

## Wann stelle ich meinen Mac wieder her?

Wenn Ihr Computer nicht mehr startet oder Sie feststellen, dass Ihr macOS (oder einige Anwendungen) nicht mehr korrekt arbeiten. In den meisten Fällen bedeutet dies, dass der Zeitpunkt gekommen ist, Ihr Betriebssystem aus einem Laufwerk-Image wiederherzustellen. Als Erstes empfehlen wir jedoch, dass Sie die Ursache Ihres Problems bestimmen.

Systemfehler beruhen zumeist auf zwei grundsätzlichen Faktoren:

- **Hardware-Fehler**
  In diesem Szenario sollten Sie die Reparatur am besten von einem Service-Center ausführen lassen.
- **Der Beschädigung eines Betriebssystems, von Anwendungen oder Daten**
  Sollte die Fehlerursache ein Virus, eine Malware oder eine Beschädigung von Systemdateien sein, dann stellen Sie das System aus einem Backup wieder her. Weitere Informationen finden Sie im Abschnitt 'Ihren Mac wiederherstellen'.

***So können Sie die Ursache Ihres Problems ermitteln***

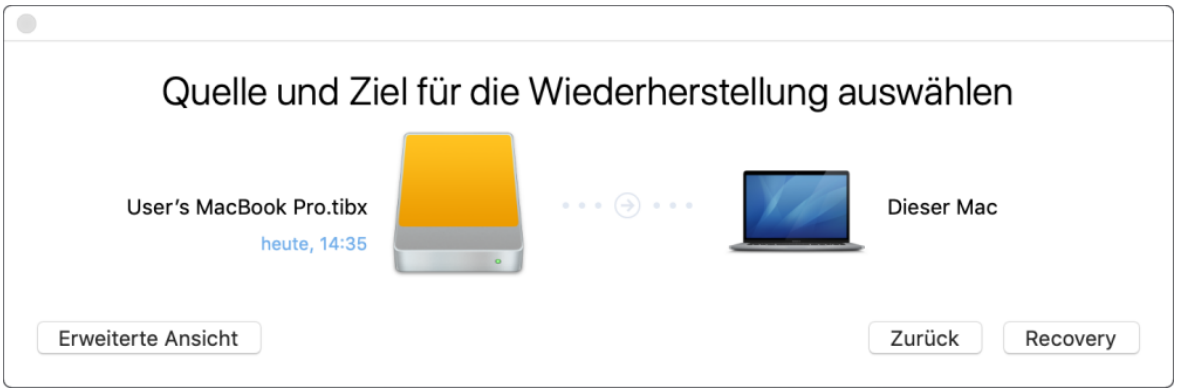
1. Überprüfen Sie Ihre Kabel, Verbindungen, die Stromversorgung Ihrer externen Geräte etc.
2. Starten Sie Ihren Mac neu. Halten Sie die **Wahltaste** gedrückt, während Ihr Mac startet. Das Menü zur Wiederherstellung wird angezeigt.
3. Wählen Sie **Festplattendienstprogramm** in der Liste und klicken Sie dann auf **Fortfahren**.
4. Wählen Sie das Festplattenlaufwerk, welches Sie überprüfen wollen, und klicken Sie dann auf den Befehl **Erste Hilfe**.
   Wenn Ihnen das Festplattendienstprogramm mitteilt, dass Ihr Laufwerk ausfallen wird, ist die Ursache im physischen Zustand der Festplatte begründet. Beispielsweise könnte Sie fehlerhafte Sektoren enthalten. Wir empfehlen, dass Sie das Festplattenlaufwerk so schnell wie möglich per Backup sichern – und dann gegen ein neues austauschen.
5. Klicken Sie auf **Volume überprüfen**.
   - Sollte ein Fehler vorliegen, dann klicken Sie auf **Volume reparieren**. Wenn das Festplattendienstprogramm meldet, dass das Laufwerk in Ordnung ist oder repariert wurde, starten Sie Ihren Mac neu und nutzen ihn weiter wie gewohnt. Sollte das Problem weiterhin bestehen, stellen Sie Ihren Mac aus einem Acronis Cyber Protect Home Office-Backup wieder her. Weitere Informationen finden Sie im Abschnitt 'Ihren Mac wiederherstellen'.
   - Falls das Festplattendienstprogramm keinen Fehler findet, stellen Sie Ihren Mac aus einem Acronis Cyber Protect Home Office-Backup wieder her. Weitere Informationen finden Sie im Abschnitt 'Ihren Mac wiederherstellen'.

# Ihren Mac wiederherstellen

Folgen Sie den unteren Anweisungen, falls Ihr Mac nicht mehr starten kann oder fehlerhaft funktioniert.

1. Stellen Sie sicher, dass Sie Folgendes haben:
   - Ein zuvor erstelltes Acronis Cyber Protect Home Office Backup. Ohne ein solches Backup ist eine Wiederherstellung nicht möglich. Details finden Sie in den Abschnitten 'Backup zu einem lokalen oder Netzwerk-Storage' und 'Backup in die Acronis Cloud'.
   - Acronis Boot-Medium. Sollten Sie noch keines haben, aber Acronis Cyber Protect Home Office auf Ihrem Mac noch starten können, dann erstellen Sie das Medium so schnell wie möglich. Weitere Informationen finden Sie im Abschnitt 'Ein Acronis Boot-Medium erstellen'.
2. Schließen Sie das Boot-Medium an Ihren Mac an.
3. So können Sie das Boot-Menü anzeigen lassen
   - [Auf einem Intel-basierten Mac] Starten Sie Ihren Mac oder führen Sie einen Neustart durch. Halten Sie die Wahltaste gedrückt, während Ihr Mac startet.
   - [Auf einem Mac mit Apple Silicon-CPU] Fahren Sie Ihren Mac herunter. Halten Sie die Einschalttaste gedrückt.
4. Wählen Sie das Acronis Boot-Medium als dasjenige Gerät aus, von dem gebootet werden soll. Das Dienstprogramm wird angezeigt.
   - [Auf einem Intel-basierten Mac] Wählen Sie die Option **Aus Acronis Cyber Protect Home Office Backup wiederherstellen** und klicken Sie dann auf **Fortfahren**.
   - [Auf einem Mac mit Apple Silicon-CPU] Wählen Sie **Acronis Boot-Medium** und klicken Sie dann auf **Wiederherstellen**.
5. Wählen Sie in dem sich öffnenden Fenster den Speicherort Ihres Backups aus:
   - **Acronis Survival Kit**
   - **Lokaler Storage**
   - **Acronis Cloud** – Melden Sie sich an Ihrem Konto an.
   - **Netzwerk**

   Wählen Sie Ihr Backup aus und klicken Sie dann auf **Öffnen**.
6. Wählen Sie aus der Liste diejenige Backup-Version, die Sie zur Wiederherstellung Ihres Macs verwenden wollen – und klicken Sie dann auf **Weiter**. Die Inhalte dieser Version werden angezeigt.
7. Aktivieren Sie die Kontrollkästchen derjenigen Volumes (hier synonym für Partitionen verwendet), die Sie wiederherstellen wollen. Bestimmen Sie für jedes Volume ein entsprechendes Ziel.




**Hinweis**
Wenn Acronis Cyber Protect Home Office ein Ziel für jedes Volume im Backup automatisch erkennt, wird die vereinfachte Ansicht angezeigt. In diesem Modus können Sie keine Änderungen vornehmen. Wenn Sie die Volumes manuell auswählen wollen, müssen Sie auf die Schaltfläche **Erweiterte Ansicht** klicken.

8. Klicken Sie zum Starten der Wiederherstellung auf **Recovery** und bestätigen Sie dann, dass alle Daten auf den Ziel-Volumes gelöscht werden sollen.
9. [Bei macOS Big Sur 11, Monterey 12, Ventura 13 und Sonoma 14] Klicken Sie bei Aufforderung auf **Daten wiederherstellen**, wenn Sie nur Daten auf einem nicht bootfähigen Daten-Volume wiederherstellen wollen. Klicken Sie auf **Mit Neustart wiederherstellen**, wenn Sie ein bootfähiges Volume mit installiertem macOS benötigen. Beachten Sie, dass dafür eine Internetverbindung erforderlich ist.
10. [Außer bei macOS Big Sur 11, Monterey 12, Ventura 13 oder Sonoma 14] Starten Sie Ihren Mac neu, sobald die Wiederherstellung abgeschlossen ist.

## FAQ über Boot Camp-Volume

- **Wie kann ich ein Backup meines Boot Camp-Volumes erstellen?**
  Erstellen Sie ein Backup des Festplattenlaufwerks, wo Boot Camp installiert ist. Dieses Backup enthält alle auf dem Laufwerk gespeicherten Daten, womit das Boot Camp-Volume eingeschlossen wäre.
- **Kann ich ein Backup allein nur von meinem Boot Camp-Volume erstellen?**
  Nein, das ist nicht möglich. Sie können mit Acronis Cyber Protect Home Office nur Backups auf Laufwerkebene erstellen. Erstellen Sie stattdessen ein Backup des gesamten Festplattenlaufwerks, auf dem das Boot Camp-Volume enthalten ist.
- **Wie kann ich mein Boot Camp-Volume wiederherstellen?**
  Sie können dies von der Betriebssystemumgebung des Boot-Mediums aus durchführen. Wählen Sie bei den Schritten für die Wiederherstellungsquelle und das Wiederherstellungsziel jeweils alle auf aufgelisteten Volumes (Partitionen) aus. Dadurch wird das komplette Festplattenlaufwerk wiederhergestellt. Wenn Sie nur das Boot Camp-Volume wiederherstellen wollen, aktivieren Sie das Kontrollkästchen neben diesem Volume und deaktivieren Sie die Kontrollkästchen aller anderen Volumes.

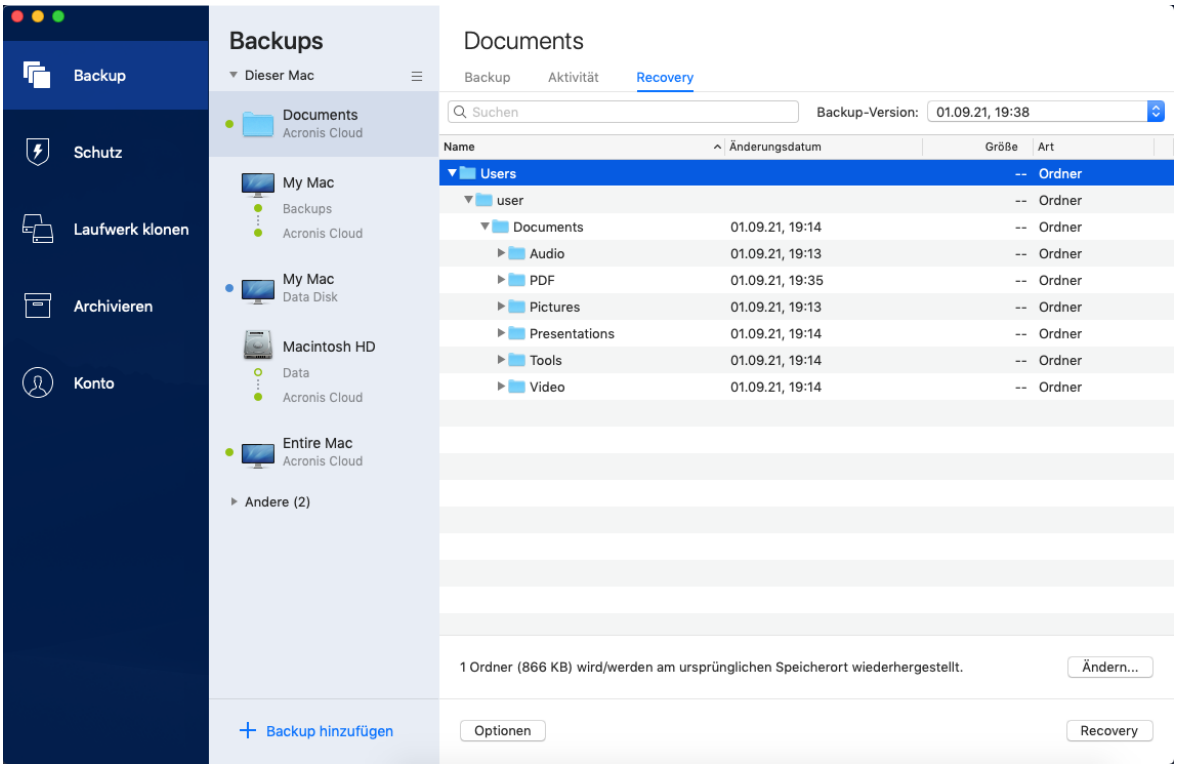
- **Kann ich die Größe meines Boot Camp-Volumes vor der Wiederherstellung anpassen?**
  Nein, das ist nicht möglich. Das Boot Camp-Volume erhält dieselbe Größe wie die im Backup vorliegende.
- **Welche Wiederherstellungsziele kann ich für ein Boot Camp-Volume wählen?**
  Sie können zwar jedes Wiederherstellungsziel wählen, jedoch empfehlen wir ausdrücklich, dass Sie Ihr Boot Camp-Volume nur auf sich selbst wiederherstellen.
- **Kann ich bestimmte Dateien aus dem Backup eines Boot Camp-Volumes wiederherstellen?**
  Ja, Sie können diese Dateien ohne Beschränkungen wiederherstellen (genauso, wie Sie auch andere Dateien wiederherstellen würden).
- **Ich möchte mein Festplattenlaufwerk durch ein neues ersetzen. Kann ich macOS, das Boot Camp-Volume und all meine Daten auf das neue Laufwerk klonen?**
  Ja, das ist möglich. Gehen Sie folgendermaßen vor:
  1. Sichern Sie Ihr Festplattenlaufwerk auf ein externen Storage (z.B. eine USB-Festplatte oder eine Netzwerkfreigabe).
  2. Schalten Sie Ihren Mac aus und tauschen Sie dann Ihr altes Festplattenlaufwerk gegen ein neues aus.
  3. Booten Sie Ihren Mac mit einem Acronis Boot-Medium.
  4. Stellen Sie Ihren Mac aus dem Backup auf das neue Festplattenlaufwerk wieder her.

# Ihre Dateien und Verzeichnisse wiederherstellen

Folgen Sie den unteren Anweisungen, wenn Sie bestimmte Dateien und Ordner aus einem Backup wiederherstellen müssen.

***So können Sie Daten in Acronis Cyber Protect Home Office wiederherstellen:***

1. Wählen Sie im linken Fensterbereich dasjenige Backup aus, welches die wiederherzustellenden Dateien und Ordner enthält – und öffnen Sie dann die Registerkarte **Recovery**.
   Das Fenster mit den Backup-Inhalten wird geöffnet.




2. Wählen Sie in der Liste **Backup-Version** die gewünschte Backup-Version anhand ihres Backup-Datums aus. Die Dateien und Ordner sind nach Abschluss der Prozedur wieder in den Zustand zurückversetzt (wiederhergestellt), in dem sie bei Erstellung des Backups vorlagen.
3. Wählen Sie die Dateien oder Ordner, die Sie wiederherstellen wollen.
4. [Optionaler Schritt] Standardmäßig werden die ausgewählten Dateien oder Ordner an ihrem ursprünglichen Speicherort wiederhergestellt. Wenn Sie einen benutzerdefinierten Speicherort als Recovery-Ziel verwenden wollen, klicken Sie zuerst auf **Ändern**. Suchen Sie anschließend aus dem Verzeichnisbaum den Speicherort aus, den Sie für die Wiederherstellung verwenden wollen.
5. [Optionaler Schritt, nur bei Cloud Backups verfügbar] Klicken Sie auf **Optionen** und konfigurieren Sie die Optionen zur Wiederherstellung von Dateien. Weitere Details finden Sie im Abschnitt 'Optionen für Datei-Recovery'.
6. Klicken Sie auf **Recovery**. Mit Abschluss des Prozesses werden Ihre Daten auf den von Ihnen gewählten Zeitpunkt hin wiederhergestellt bzw. zurückgesetzt und am ursprünglichen oder einem benutzerdefinierten Speicherort abgelegt.

   Bei einem Notarized Backup wird Acronis Cyber Protect Home Office zusätzlich die Authentizität der wiederhergestellten Dateien überprüfen.

***So können Sie Daten von der Acronis Cloud aus wiederherstellen***

Sie können bestimmte Dateien und Ordner aus einem Online Backup wiederherstellen, welches in der Acronis Cloud gespeichert ist.Zur Durchführung dieser Aktion müssen Sie zuerst die Acronis Cloud Website aufrufen.

***So können Sie die Acronis Cloud Website öffnen***

– Auf Ihrem Mac, auf dem Acronis Cyber Protect Home Office installiert ist

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Klicken Sie im linken Fensterbereich auf **Konto**.
3. Wählen Sie im Acronis Cyber Protect Home Office-Bereich den Befehl **Meine Daten durchsuchen**.

– Auf einem Computer oder Mobilgerät mit bestehender Internetverbindung:

1. Gehen Sie mit Ihrem Webbrowser zur Adresse 'https://www.acronis.com/my/online-backup/webrestore/'.
2. Melden Sie sich an Ihrem Acronis Konto an.

Die Acronis Cloud-Webseite wird in Ihrem Webbrowser geöffnet.

***So können Sie Dateien und Ordnern wiederherstellen***

1. Klicken Sie in der Registerkarte **Backups** der Acronis Cloud-Webseite auf den gewünschten Backup-Namen. Lokalisieren Sie dann die Dateien oder Ordner, die Sie wiederherstellen wollen. Sie können auch das Feld **Suchen** verwenden. Wählen Sie die gewünschte Datei oder den gewünschten Ordner über das entsprechende Kontrollkästchen aus.
2. [Optional] Wenn Sie von einer Datei (gilt nicht für Ordner) eine bestimmte Version wiederherstellen wollen, klicken Sie in der rechten Seitenleiste auf **Versionen**. Wählen Sie dann den gewünschten Zeitpunkt (Datum, Uhrzeit) des Backups aus und klicken Sie dann auf das Download-Symbol in dieser Zeile.
3. Klicken Sie zum Starten der Wiederherstellung auf **Download**.

Die ausgewählten Daten werden in den vorgegebenen Download-Ordner heruntergeladen.

# Microsoft 365-Daten wiederherstellen

Mit Acronis Cyber Protect Home Office können Sie Ihr persönliches Microsoft 365-Konto per Backup davor schützen, dass Sie Ihre E-Mail-Nachrichten, Dateien und Ordner, Profil-Informationen und andere Daten verlieren. Wenn Sie Ihre Kontodaten per Cloud Backup gesichert haben, können Sie das Backup bei Bedarf in der Cloud durchsuchen und dabei einzelne Elemente direkt wiederherstellen.

## Welche Elemente können wiederhergestellt werden?

**Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:**

- Komplettes Postfach
- E-Mail-Nachrichten
- Anhänge

**Folgende Elemente können aus einem OneDrive-Backup wiederhergestellt werden:**

- Kompletter OneDrive-Ordner
- Alle Dateien und Ordner, die im Backup gesichert wurden

## Microsoft 365-Daten wiederherstellen

***So können Sie Ihre Daten durchsuchen und wiederherstellen***

1. Öffnen Sie das Online Dashboard durch eine der folgenden Aktionen:
   - Folgen Sie diesem Link: https://cloud.acronis.com.
   - Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office auf den Befehl **Konto** und anschließend auf **Online Dashboard öffnen**.
2. Melden Sie sich an Ihrem Acronis Konto an.
3. Klicken Sie in der Seitenleiste auf **Ressourcen**, suchen Sie das Microsoft 365-Backup und klicken Sie dann auf **Recovery**.
4. Durchsuchen Sie die Liste Ihrer Backups. Verwenden Sie bei Bedarf die Filterfunktion, um bestimmte Inhalte im Backup zu finden.
5. Klicken Sie nach der Auswahl des Backups auf **Wiederherstellen...** und bestimmen Sie, welche Daten genau Sie wiederherstellen wollen:
   - Das komplette OneDrive oder bestimmte Dateien bzw. Ordner.
   - Das komplette Postfach oder bestimmte Nachrichten.

   Wenn Sie sich zur Wiederherstellung bestimmter Elemente entschlossen haben, wird das Online Dashboard eine Liste der gesicherten Elemente öffnen. Sie können diese nun durchsuchen, die entsprechende Inhalte anzeigen lassen und eine Suchfunktion benutzen, um bestimmte Elemente zu finden (wird nicht für alle Datentypen unterstützt).

   Nachdem Sie die Elemente ausgewählt haben, können Sie bestimmen, welche Aktion(en) mit diesen durchgeführt werden soll (je nach Datentyp sind einige Aktionen nicht verfügbar):
   - **Inhalt anzeigen** – mit diesem Befehl werden Elementinformationen angezeigt oder das Element im Vollbild geöffnet.
   - **Als E-Mail senden** – mit diesem Befehl können Sie die Nachricht an bestimmte Empfänger übermitteln.
   - **Versionen anzeigen** – mit diesem Befehl können Sie sich die Versionen des Elements anzeigen lassen.
   - **Recovery** – mit diesem Befehl können Sie den Zielspeicherort für die wiederherzustellenden Elemente festlegen. Für einige Elemente können Sie auch Freigabe-Berechtigungen wiederherstellen.
   - **Download** – mit diesem Befehl können Sie eine ausgewählte Datei herunterladen.
6. Klicken Sie auf **Recovery starten**.

# Backup-Inhalte durchsuchen

Wenn Sie Daten aus einem lokalen Backup wiederherstellen, können Sie eine Suchfunktion verwenden, um bestimmte Dateien/Ordner zu finden, die im ausgewählten Backup gespeichert sind.

***So können Sie nach Dateien und Ordnern suchen***

1. Starten Sie eine Datenwiederherstellung wie im Abschnitt 'Dateien aus einem lokalen oder Netzwerk-Storage wiederherstellen' beschrieben.
2. Geben Sie bei der Auswahl der wiederherzustellenden Dateien/Ordner den gewünschten Datei-/Ordnernamen in das Feld **Suche** ein. Das Programm zeigt daraufhin Suchergebnisse an.
   Sie können außerdem diese Platzhalterzeichen (Wildcards) verwenden: '*' und '?'. Wenn Sie beispielsweise alle Dateien mit der Erweiterung **.exe** finden möchten, geben Sie ***.exe** ein. Mit der Eingabe **Meine???.exe** werden alle Dateien mit der Erweiterung '.exe' gefunden, die aus acht Zeichen bestehen und zudem mit 'Meine' beginnen.
3. Acronis Cyber Protect Home Office durchsucht standardmäßig den im vorherigen Schritt ausgewählten Ordner. Wenn Sie Backup vollständig durchsuchen wollen, klicken Sie auf **Komplettes Backup**.
   Klicken Sie auf das Symbol mit dem Kreuz, um zum vorherigen Schritt zurückzukehren.
4. Wenn die Suche abgeschlossen wurde, können Sie die wiederherzustellenden Dateien auswählen und auf **Weiter** klicken.

**Hinweis**
Achten Sie auf die Spalte **Version**. Dateien und Ordner, die zu unterschiedlichen Backup-Versionen gehören, können nicht gleichzeitig wiederhergestellt werden.

# Optionen für Datei-Recovery

Sie können folgende Dateiwiederherstellungsoptionen für Backups auswählen:

- **Dateiberechtigungen bewahren** – diese Option wird alle Sicherheitseinstellungen (Benutzerberechtigungen für Gruppen oder Benutzer) der gesicherten Dateien erhalten. Standardmäßig werden Dateien und Ordner im Backup mit ihren ursprünglichen Sicherheitseinstellungen (d.h. Lese-, Schreib- und Ausführungsrechte etc. für jeden Benutzer) gespeichert. Wenn Sie Dateien/Ordner auf einem Computer wiederherstellen, die unter einem anderen Benutzerkonto gesichert wurden, werden Sie möglicherweise nicht mehr in der Lage sein, diese Dateien/Ordner zu lesen oder zu verändern.
  Wenn Sie diese Option deaktivieren und Dateien im vorliegenden Standard-Benutzerordner wiederherstellen, wird der aktuelle Benutzer zum Besitzer der wiederhergestellten Dateien/Ordner.
- **Vorhandene Dateien überschreiben** (nur für Cloud Backups auf Dateiebene verfügbar) – wenn Sie diese Option wählen, werden die Dateien auf dem Laufwerk mit den Dateien aus dem Backup

überschrieben, sofern sich die Dateien unterscheiden. Wenn Ihre Dateien/Ordner über neuere Änderungen verfügen, die Sie beim Wiederherstellen beibehalten wollen, dann wählen Sie die Option **Neuere Dateien und Ordner nicht überschreiben**.

# Schutz

Acronis Cyber Protect Home Office bietet folgende Arten von Schutz:

- Active Protection wird kontinuierlich im Hintergrund ausgeführt, um Ihre Maschinen in Echtzeit zu schützen, während Sie wie gewohnt arbeiten können.
- Antivirus-Scans werden bei Bedarf („On-Demand“) ausgeführt, um eine gründliche Suche nach Schadsoftware im gesamten System durchzuführen.
- Die Schwachstellenbewertung ist ein täglicher, im Hintergrund ausgeführter Scan, der Schwachstellen (wie Sicherheitslücken) in Ihrem System und Ihren Applikationen erkennen kann und dann deren Schweregrad bewerten.

**Hinweis**
Sie können den Schutz nur über die Benutzeroberfläche von Acronis Cyber Protect Home Office ein- bzw. ausschalten. Es ist dagegen nicht möglich, den Prozess manuell (über den Activity Monitor oder ein anderes, externes Tool) zu stoppen.

## Das Protection Dashboard

Das Protection Dashboard enthält statistische Daten, ermöglicht die Kontrolle über den Schutzstatus sowie den Zugriff auf die Schutzeinstellungen.

Wenn Sie auf das Protection Dashboard zugreifen wollen, klicken Sie in der Seitenleiste von auf **Schutz**.

In der Registerkarte **Überblick** des Dashboards können Sie Folgendes tun:

- Statistiken über den aktiven Schutzstatus einsehen.
- Die Anzahl der erkannten Probleme und der unter Quarantäne gestellten Elemente einsehen.
- Den letzten Bericht über den **Antivirus-Scan** einsehen.
- Die nächste geplante Scanzeit einsehen.
- Manuell einen vollständigen **Antivirus-Scan** durchführen. Klicken Sie dafür auf **Vollständigen Scan ausführen**.
- Den jüngsten Bericht über erkannte Schwachstellen einsehen und einen neuen Scan ausführen.
- Den gesamten Schutz für eine vordefinierte Zeitspanne (30 Minuten, 1 Stunde, 4 Stunden, bis zum Neustart) stoppen. Klicken Sie dafür auf **Schutz ausschalten** und wählen Sie den gewünschten Zeitraum aus.

  **Hinweis**
  Wenn Sie den Schutz pausieren, wird die Active Protection-Funktionalität deaktiviert. Geplante On-Demand-Scans werden nicht mehr gestartet.

Auf der Registerkarte **Aktivität** des Dashboards können Sie ein Protokoll derjenigen Änderungen einsehen, die Sie an Ihrem Schutzstatus und Ihren Einstellungen vorgenommen haben.

# Active Protection

Acronis Cyber Protect Home Office verwendet die Acronis Active Protection-Technologie, um Ihre Dateien vor bösartiger Software zu schützen.

Active Protection überprüft Ihren Computer, während Sie wie gewohnt weiterarbeiten können. Zusätzlich zu Ihren Dateien schützt Acronis Active Protection außerdem die Applikationsdateien von Acronis Cyber Protect Home Office sowie Ihre Backups.

Active Protection besteht aus zwei Schutzstufen, die Sie unabhängig voneinander aktivieren können:

- Anti-Ransomware Protection
- Echtzeitschutz

## Anti-Ransomware Protection

Ransomware verschlüsselt Dateien und verlangt ein Lösegeld für die Bereitstellung des Codierungsschlüssels.

Wenn der **Antiransomware Protection** Service eingeschaltet ist, überwacht er in Echtzeit die auf Ihrem Computer laufenden Prozesse. Wenn der Service erkennt, dass ein fremder Prozess Ihre Dateien verschlüsseln möchte, werden Sie vom Service informiert und gefragt, ob der Prozess seine Aktivität fortsetzen darf oder Sie ihn blockieren wollen.

Klicken Sie auf **Vertrauen**, wenn Sie dem Prozess erlauben wollen, seine Aktivität fortzusetzen. Falls Sie sich nicht sicher sind, ob der Prozess sicher und zulässig ist, empfehlen wir, auf **Quarantäne** zu klicken. Danach wird der Prozess in die **Quarantäne** verschoben und jede seiner Aktivitäten blockiert.

### Ihre Dateien wiederherstellen, wenn ein Prozess blockiert wurde

Sollten Sie einen Prozess blockiert haben, so empfehlen wir, dass Sie anschließend Ihre Dateien darauf überprüfen, ob diese verschlüsselt oder irgendwie beschädigt wurden. Wenn sie das tatsächlich sind, können Sie auf **Geänderte Dateien wiederherstellen** klicken. Acronis Cyber Protect Home Office wird die nachfolgenden Speicherorte nach den neuesten Dateiversionen zur Wiederherstellung durchsuchen.

- Temporärer Dateikopien, die zuvor bei der Prozess-Verifizierung erstellt wurden
- Lokale Backups
- Cloud Backups

Wenn Acronis Cyber Protect Home Office eine gute temporäre Kopie findet, wird die ursprüngliche Datei mithilfe dieser Kopie wiederhergestellt. Wenn die temporäre Dateikopien für die Wiederherstellung nicht geeignet sein sollten, sucht Acronis Cyber Protect Home Office nach Backup-Kopien, vergleicht die Erstellungszeiten der gefundenen Kopien und wird dann Ihre Datei von der letzten verfügbaren, unbeschädigten Kopie wiederherstellen.

**Hinweis**
Acronis Cyber Protect Home Office unterstützt keine Dateiwiederherstellung aus kennwortgeschützten Backups.

## Echtzeitschutz

Wenn der **Echtzeitschutz** aktiviert ist, überprüft dieser kontinuierlich alle Dateien, mit denen Sie interagieren, um Ihre Maschine in Echtzeit vor verdächtigen Aktivitäten, Viren und anderen bösartigen Bedrohungen zu schützen.

Der Echtzeitschutz hat zwei Betriebsmodi:

- **Bei Zugriff (intelligent)** – alle Systemaktivitäten werden überwacht und die Dateien werden gescannt, sobald Sie auf diese zugreifen.
- **Bei Ausführung** – es werden nur ausführbare Dateien gescannt – und zwar, wenn diese gestartet werden. Dadurch wird sichergestellt, dass diese Dateien Ihre Maschine nicht beschädigen können.

Sie können den Echtzeitschutz dahingehend konfigurieren, was mit blockierten Dateien geschehen soll:

- **Blockieren und unter Quarantäne stellen** – Der Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, wird blockiert und die entsprechende Datei wird in den Quarantäne-Ordner verschoben.
- **Blockieren und benachrichtigen** – Der Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, wird blockiert und Sie erhalten eine Benachrichtigung darüber.

Sie können die Ergebnisse in der Liste der **Aktivitäten** einsehen.

## Active Protection konfigurieren

***So können Sie die Antiransomware Protection konfigurieren***

1. Klicken Sie zuerst in der Seitenleiste von Acronis Cyber Protect Home Office auf **Schutz** und dann auf **Einstellungen**.
2. Gehen Sie zur Registerkarte **Active Protection** und aktivieren Sie die **Antiransomware Protection**.

Sobald der Schalter aktiviert wurde, schützt die Antiransomware Protection Ihren Computer vor potenziell schädlichen Applikationen und Hintergrund-Prozessen.

***So können Sie den Echtzeitschutz konfigurieren***

1. Klicken Sie zuerst in der Seitenleiste von Acronis Cyber Protect Home Office auf **Schutz** und dann auf **Einstellungen**.
2. Gehen Sie zur Registerkarte **Active Protection** und aktivieren Sie den **Echtzeitschutz**.

Wenn die Funktion aktiviert wird, überprüft der Echtzeitschutz alle Dateien, mit denen Sie interagieren, auf Malware.

3. Wählen Sie aus, wann die Dateien überprüft werden sollen.
   - **Bei Zugriff (intelligent)** – Alle Systemaktivitäten werden überwacht und die Dateien werden gescannt, sobald Sie auf diese zugreifen.
   - **Bei Ausführung** – Es werden nur ausführbare Dateien gescannt - und zwar, wenn diese gestartet werden. Dadurch wird sichergestellt, dass diese Dateien Ihre Maschine nicht beschädigen können.
4. Bestimmen Sie, was mit den erkannten Objekten geschehen soll.
   - **Blockieren und benachrichtigen** – Der Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, wird blockiert und Sie erhalten eine Benachrichtigung darüber.
   - **Blockieren und unter Quarantäne stellen** – Der Prozess, bei dem der Verdacht auf Malware-Aktivität besteht, wird blockiert und die ausführbare Datei wird in den Quarantäne-Ordner verschoben.
5. Klicken Sie auf **OK**.

# Identitätsschutz

**Wichtig**
Der Identitätsschutz ist derzeit nur für die Advanced- und Premium-Lizenzen verfügbar. Eine Liste der Länder, in denen diese Funktion unterstützt wird, finden Sie in diesem Knowledge Base-Artikel.

Der Identitätsschutz ist eine Zusammenstellung von Maßnahmen, die verhindern, dass Cyberkriminelle Ihre persönlichen Daten stehlen. Dabei werden folgende Informationen überwacht:

- Grundlegende Daten wie die Personalausweisnummer, Reisepässe, Führerscheine, Adressen, Telefonnummern, E-Mail-Adressen und Anmeldedaten
- Finanzielle Informationen über Zahlungskarten und Bankkonten
- Versicherungsunterlagen, wie Dokumente zur Kranken- und Kfz-Versicherung

Diese Informationen könnten infolge einer Datenschutzverletzung, eines Phishing- oder Malware-Angriffs entwendet bzw. offengelegt werden. Der Identitätsschutz hilft Ihnen, solche Datenexpositionen und andere verdächtige Aktivitäten im Zusammenhang mit Ihren Informationen zu erkennen. Im dafür vorgesehenen Identity Protection Dashboard können Sie Folgendes tun:

- Ihre persönlichen Informationen, die überwacht werden sollen, hinzufügen und aktualisieren
- Die Sicherheit Ihrer Daten überwachen
- Alarmmeldungen über Datenexpositionen konfigurieren
- Unterstützung bei Identitätsdatendiebstahl anfordern Sie können das Support-Team auch über support@info.idprotectiononline.com kontaktieren.
- Rückerstattung bei Identitätsdatendiebstahl anfordern

***So können Sie den Identitätsschutz zum ersten Mal konfigurieren***

1. Klicken Sie in der linken Seitenleiste von Acronis Cyber Protect Home Office auf **Schutz**.
2. Klicken Sie unter **Identitätsschutz** auf **Schutz verwalten**. Das Online Dashboard wird im Browser geöffnet. Weitere Informationen finden Sie im Abschnitt '"Was ist das Online Dashboard?" (S. 79)'
3. Melden Sie sich am Online Dashboard an.
4. Klicken Sie auf der Registerkarte **Identitätsschutz** auf **Schutz verwalten**.
5. Geben Sie im Fenster **Geben Sie Ihre Identitätsdaten ein** Ihre persönlichen Informationen ein.

   **Wichtig**
   Überprüfen Sie, dass die Informationen vollständig und korrekt sind. Anderenfalls kann es sein, dass Sie nicht benachrichtigt werden, wenn Ihre tatsächlichen Identitätsdaten gefährdet sind.

   Sobald Sie die Daten eingegeben haben, beginnen wir damit, die Sicherheit Ihrer Daten regelmäßig zu überprüfen.
6. Das Identity Protection Dashboard wird in Ihrem Browser geöffnet.

***So können Sie das Identity Protection Dashboard von Acronis Cyber Protect Home Office aus öffnen***

1. Klicken Sie in der linken Seitenleiste von Acronis Cyber Protect Home Office auf **Schutz**.
2. Klicken Sie unter **Identitätsschutz** auf **Schutz verwalten**.
   Das Online Dashboard wird im Browser geöffnet.
3. Melden Sie sich am Online Dashboard an.
4. Klicken Sie auf der Registerkarte **Identitätsschutz** auf **Schutz verwalten**.
5. Das Identity Protection Dashboard wird im Browser geöffnet.

***So können Sie das Identity Protection Dashboard vom Online Dashboard aus öffnen***

1. Öffnen Sie das Online Dashboard über die Adresse https://cloud.acronis.com. Weitere Informationen finden Sie im Abschnitt '"Was ist das Online Dashboard?" (S. 79)'
2. Klicken Sie in der linken Seitenleiste des Online Dashboards auf **Schutz** –> **Identitätsschutz**.
3. Klicken Sie auf der Registerkarte **Identitätsschutz** auf **Schutz verwalten**.
4. Das Identity Protection Dashboard wird in Ihrem Browser geöffnet.

# Antivirus-Scans

Die **Antivirus-Scan**-Funktionalität ist eine der Komponenten der Acronis Cyber Protect Home Office Antivirus & Antimalware Protection. Sie schützt Ihren Computer, indem sie bei Bedarf („On-Demand“) nach Malware sucht – manuell oder in vordefinierten Zeitintervallen, die Sie konfigurieren können.

Sie können zwischen zwei Scan-Varianten wählen.

- Ein **Vollständiger** Scan durchsucht die komplette Maschine nach Viren. Ein vollständiger Scan erkennt Malware, indem alle Dateien und Prozesse (oder eine Teilmenge von diesen) untersucht werden – mit Ausnahme solcher Dateien oder Ordner, die Sie in Form von Ausschlusslisten definieren können.
- Ein **Schnellscan** untersucht nur bestimmte Dateien und Ordner. Ein Schnellscan erkennt Malware, indem er bestimmte Ordner untersucht, die als gängige Speicherorte für Viren bekannt sind.

Sie können auch bestimmen, was gescannt werden soll: Archivdateien, externe Laufwerke oder nur neue sowie geänderte Dateien.

**Hinweis**
Sie können Acronis Cyber Protect Home Office so konfigurieren, dass Ihr Computer nicht in den Energiesparmodus wechselt, wenn eine Scan-Aktion läuft. Beachten Sie, dass diese Option standardmäßig aktiviert ist.

Die Priorität eines Antivirus-Scans wird standardmäßig herabgesetzt, wenn es während seiner Ausführung zu einer hohen CPU-Last kommt, damit alle anderen Applikationen ungestört weiterarbeiten können. Wenn Sie das Scannen unter diesen Umständen beschleunigen wollen, können Sie diese Option auch deaktivieren.

Sie können sich die **Antivirus-Scan**-Ergebnisse im **Scan-Details-Bericht** anzeigen lassen.

## Antivirus-Scans konfigurieren

1. Klicken Sie zuerst in der Seitenleiste von Acronis Cyber Protect Home Office auf **Schutz** und dann auf **Einstellungen**.
2. Gehen Sie zur Registerkarte **Antivirus** und wenden Sie die gewünschten Einstellungen an.
3. Wenn Sie den Scan-Typ konfigurieren wollen, aktivieren Sie in der Registerkarte **Planung** das erforderliche Kontrollkästchen.
   - **Vollständig** – Diese Option ist standardmäßig festgelegt. Acronis Cyber Protect Home Office wird den kompletten Mac überprüfen.
   - **Schnell** – Acronis Cyber Protect Home Office wird nur solche Ordner prüfen, die als gängige Speicherorte für Bedrohungen gelten.
4. Wenn Sie Antivirus-Scans planen wollen, müssen Sie auf der Registerkarte **Planung** die erforderlichen Kontrollkästchen aktivieren, um den Zeitpunkt zu konfigurieren, an dem der Scan-Prozess starten soll.
   - **Ohne Planung** – Für die Scan-Ausführung wird kein bestimmter Zeitpunkt geplant.
   - **Täglich** – Der Scan wird jeden Tag am spezifizierten Zeitpunkt durchgeführt. Legen Sie die Uhrzeit fest.
   - **Wöchentlich** – Der Scan wird an einem bestimmten Wochentag ausgeführt. Legen Sie den gewünschten Wochentag und die Uhrzeit fest.

- **Monatlich** – Der Scan wird an einem bestimmten Tag des Monats ausgeführt.
- **Beim Systemstart** – Der Scan wird bei jedem Start Ihres Betriebssystems ausgeführt.

5. Wenn Sie eine 'Aktion bei Erkennung' konfigurieren wollen, müssen aktivieren Sie in der Registerkarte **Optionen** die erforderlichen Kontrollkästchen aktivieren.
   - **Quarantäne** – Diese Option ist standardmäßig festgelegt. Wenn Acronis Cyber Protect Home Office eine potenzielle Malware-Bedrohung erkennt, stoppt es den entsprechenden Prozess und verschiebt dann die verdächtige Datei in den Quarantäne-Ordner.
   - **Nur benachrichtigen** – Wenn ein verdächtiger Prozess erkannt wird, erhalten Sie eine Benachrichtigung über die potenzielle Malware-Bedrohung.
6. Wenn Sie konfigurieren wollen, was gescannt werden soll, müssen Sie in der Registerkarte **Optionen** die erforderlichen Kontrollkästchen aktivieren.
   - **Archivdateien scannen**
   - **Externe Laufwerke scannen**
   - **Netzwerkfreigaben und NAS-Geräte scannen**
   - **Nur neue und geänderte Dateien scannen**
7. Wenn Sie das Systemverhalten während der Antivirus-Scans konfigurieren wollen, aktivieren Sie die erforderlichen Kontrollkästchen.
   - **Standby- oder Ruhezustandsmodus verhindern** – Ihr Computer wird nicht heruntergefahren, solange der Scan nicht abgeschlossen wurde.
   - **Verpasste Tasks bei Neustart ausführen** – Wenn einige Tasks noch nicht abgeschlossen waren, bevor das System heruntergefahren wurde, wird der Scan-Prozess beim Neustart des Systems wieder fortgesetzt.
   - **Anderen Applikationen Priorität geben** – Für den Fall, dass die CPU bei einem Scan mal überlastet sein sollte, kann die Priorität der Antivirus-Scans heruntergestuft werden, damit andere Applikationen in so einer Situation weiter korrekt arbeiten können. Dieses Kontrollkästchen ist standardmäßig aktiviert, was jedoch dazu führen kann, dass das Scannen mehr Zeit benötigt.
8. Klicken Sie nach der Konfiguration der Antivirus-Scan-Optionen auf **OK**, damit Ihre Änderungen übernommen werden.

Sie können sich die Antivirus-Scan-Ergebnisse im **Scan-Details-Bericht** anzeigen lassen.

# Schwachstellenbewertung

Die Schwachstellenbewertung ist eine (von mehreren) Komponenten der Acronis Cyber Protect Home Office Antivirus & Antimalware Protection. Es handelt sich um einen täglichen, im Hintergrund ausgeführten Scan, der Schwachstellen (wie Sicherheitslücken) in Ihrem System und Ihren Applikationen erkennen kann und dann deren Schweregrad bewerten. Sie können den Scan bei Bedarf auch manuell ausführen.

**Hinweis**
Für die Schwachstellenbewertung ist eine stabile Internetverbindung erforderlich.

***So können Sie sich die Schwachstellen anzeigen lassen:***

1. Klicken Sie in der linken Seitenleiste auf **SCHUTZ**.
2. Klicken Sie in der Registerkarte **Überblick** unter **Schwachstellenbewertung** auf **Erkannte Schwachstellen**. Der entsprechende Bericht wird angezeigt.
3. Wenn Sie einen neuen Scan ausführen wollen, müssen Sie auf **Scan ausführen** klicken.
4. [optional] Wenn Sie ausführliche Informationen zu einer Schwachstelle in Acronis Cyber Protect Home Office einsehen wollen, klicken Sie neben dem Namen der betreffenden Schwachstelle auf den Pfeil. Das Fenster **Ausführliche Informationen** wird geöffnet und zeigt Details zur entsprechenden Schwachstelle an – beispielsweise, welche Produktversion betroffen ist.
5. [optional] Wenn Sie weitere Informationen über eine Schwachstelle einsehen wollen:
   - Klicken Sie im Bericht neben dem Namen der Schwachstelle auf das Symbol **i**.
   - Klicken Sie im Fenster **Ausführliche Informationen** auf **Mehr Informationen**.

   Daraufhin wird eine Webseite mit einer ausführlichen Beschreibung der Schwachstelle angezeigt.
6. Wenn Sie die erkannten Probleme beheben wollen, müssen Sie die neuesten Updates für die betroffenen Applikationen installieren. Danach sollten Sie einen erneuten Scan durchführen, um zu überprüfen, dass die Schwachstellen auch wirklich behoben wurden. Wenn diese weiterhin bestehen, bedeutet dies, dass Ihr System immer noch durch einige Applikationen gefährdet ist. Wenn Sie Ihre Daten umfassend schützen wollen, sollten Sie Ihre komplette Maschine per Backup sichern und die Antimalware Protection einschalten.

***So können Sie die Schwachstellenbewertung konfigurieren:***

1. Klicken Sie in der linken Seitenleiste auf **SCHUTZ** und anschließend auf **Einstellungen**.
2. Gehen Sie zur Registerkarte **Schwachstellenbewertung** und verwenden Sie das entsprechende Kontrollkästchen, um den Schwachstellen-Scan je nach Bedarf zu aktivieren oder zu deaktivieren.

# Laufwerk klonen

## Das Werkzeug 'Laufwerk klonen'

**Hinweis**
Bestimmte Programmfunktionen sind in der von Ihnen verwendeten Edition möglicherweise nicht verfügbar.

Eine gewöhnliche Kopier-Aktion bewirkt nicht, dass Ihr neues Laufwerk mit dem alten identisch ist. Wenn Sie beispielsweise den Finder öffnen würden, um alle Dateien und Ordner auf das neue Laufwerk zu kopieren, würde macOS von dem neuen Laufwerk nicht starten können. Das Werkzeug 'Laufwerk klonen' ermöglicht Ihnen, all Ihre Daten zu duplizieren und macOS auf dem neuen Laufwerk bootfähig zu machen. Dadurch wird Ihre neue Festplatte zu einem exakten Klon Ihres alten Laufwerks.

**Einsatzszenario:**

- Sie haben einen neuen iMac oder ein MacBook gekauft und wollen alle Ihre Daten (einschließlich dem Betriebssystem) von Ihrem alten Mac auf den neuen übertragen.
- Sie möchten ein externes Laufwerk zu einem tragbaren Klon der Festplatte Ihres Macs machen. Sie können dieses externe Laufwerk an einen beliebigen anderen Mac anschließen und booten, wodurch dieser Mac sofort zu einer exakten Kopie Ihres eigenen Macs wird.

**Welche Laufwerke Sie verwenden können:**

- Das interne Systemlaufwerk Ihres Macs (kann nur als Quelllaufwerk verwendet werden)
- Ein internes Laufwerk Ihres Macs, das kein Systemlaufwerk ist
- Das interne Laufwerk eines anderen Macs
- Ein externes Laufwerk
- Einen USB-Stick

Wenn das Ziellaufwerk größer oder kleiner als das Quelllaufwerk ist, wird die Größe der Quelllaufwerk-Volumes auf dem Ziellaufwerk proportional so angepasst, dass diese den kompletten Speicherplatz des Ziellaufwerks belegen. Davon ausgenommen sind lediglich Volumes (Partitionen), die kleiner als 1 GB sind. Die Größe dieser Volumes wird nicht angepasst.

Das Ziellaufwerk muss nicht die gleiche Größe wie das Quelllaufwerk haben, sondern es kann auch kleiner oder größer sein. Seine Gesamtgröße muss jedoch größer als der belegte Speicherplatz des Quelllaufwerks plus 10% sein. Beispiel: Sie haben einen Mac mit einer 1000-GB-Festplatte, von denen aber nur 200 GB verwendet werden. Wenn Sie dieses Laufwerk klonen wollen, muss die Größe des Ziellaufwerks mindestens 200+10% = 220 GB betragen – oder größer sein. Wenn Ihr Ziellaufwerk zu klein ist, sollten Sie nicht mehr benötigte Daten vom Quelllaufwerk löschen oder weniger benötigte Daten auf eine externe Festplatte oder einen USB-Stick verschieben. Sie können die Daten auch in den Cloud Storage verschieben.

# Laufwerke klonen

Eine gewöhnliche Kopier-Aktion bewirkt nicht, dass Ihr neues Laufwerk mit dem alten identisch ist. Wenn Sie beispielsweise den Finder öffnen würden, um alle Dateien und Ordner auf das neue Laufwerk zu kopieren, würde macOS von dem neuen Laufwerk nicht starten können. Das Werkzeug 'Laufwerk klonen' ermöglicht Ihnen, all Ihre Daten zu duplizieren und macOS auf dem neuen Laufwerk bootfähig zu machen. Dadurch wird Ihre neue Festplatte zu einem exakten Klon Ihres alten Laufwerks. Weitere Details finden Sie im Abschnitt 'Das Werkzeug 'Laufwerk klonen''.

**Wichtig**
Wenn Sie einen Mac mit Apple Silicon-Architektur (mit M1- oder M2-Chip) klonen wollen, müssen Sie die Daten zuerst zu einem externen Laufwerk klonen. Danach müssen Sie die Daten von diesem externen Laufwerk auf den als Ziel dienenden Mac übertragen.

***So können Sie ein Laufwerk klonen***

1. Wenn auf Ihrem Mac virtuelle Maschinen (VMs) von Parallels Desktop laufen, sollten Sie sicherstellen, dass diese heruntergefahren sind.
2. Überprüfen Sie, dass die Quell- und Ziellaufwerke mit Ihrem Mac verbunden sind. Wenn Sie einen anderen Mac anschließen müssen, sollten Sie sicherstellen, dass dieser im Festplattenmodus angeschlossen ist. Weitere Informationen finden Sie im Abschnitt 'Zwei Macs verbinden'.
3. Öffnen Sie Acronis Cyber Protect Home Office.
4. Klicken Sie in der Seitenleiste auf **Laufwerk klonen** und dann auf **Fortsetzen**.
5. Standardmäßig wird Ihr internes Systemlaufwerk als Quelle für die Klonen-Aktion vorausgewählt. Sie können dies aber ändern, indem Sie auf das Symbol für die Klon-Quelle klicken und dann dasjenige Laufwerk auswählen, welches Sie stattdessen klonen wollen.
6. Schließen Sie das Ziellaufwerk an.

   **Hinweis**
   Die Aktion 'Laufwerk klonen' wird nicht für APM-Laufwerke oder Laufwerke, die mit SoftRAID initialisiert wurden, unterstützt. Wenn Sie ein APM-Laufwerk haben, empfehlen wir, dass Sie dessen Partitionstyp von GPT zu MBR konvertieren.

7. Klicken Sie auf das Symbol für das Ziellaufwerk und wählen Sie dann dasjenige Laufwerk aus, welches als Ziel für die zu klonenden Daten fungieren soll.

   **Warnung!**
   Wenn Sie die Klonen-Aktion starten, wird das Ziellaufwerk formatiert, sodass alle darauf gespeicherten Daten unwiderruflich gelöscht werden. Überprüfen Sie, dass das Laufwerk leer ist oder keine wertvollen Daten enthält.

8. Klicken Sie auf **Klonen**.

***Zusätzliche Schritte bei einem Mac mit Apple Silicon-Architektur (mit M1- oder M2-Chip)***

1. Verbinden Sie das Klon-Laufwerk mit dem Ziel-Mac.
2. Fahren Sie Ihren Ziel-Mac herunter und halten Sie dann die **Einschalttaste** so lange gedrückt, bis Ihnen die Startoptionen angezeigt werden.
3. Klicken Sie zum Konfigurieren der macOS-Wiederherstellung auf **Optionen**.
4. Wählen Sie **Festplattendienstprogramm** aus. Wählen Sie in der Werkzeugleiste die Option **Alle Geräte einblenden**.
5. Wählen Sie das interne Laufwerk Ihres Macs aus und klicken Sie in der Werkzeugleiste auf **Löschen**. Wählen Sie das APFS-Format und bestätigen Sie das Löschen. Danach wird Ihr Mac neu gestartet.
6. Aktivieren Sie Ihren Mac. Beenden Sie den Vorgang und wechseln Sie zu den Wiederherstellungsdienstprogrammen.
7. Wählen Sie, dass macOS erneut installiert werden soll, und befolgen Sie dann die angezeigten Schritte, um macOS auf dem internen Laufwerk zu installieren.
8. Wenn macOS zum ersten Mal startet, konfigurieren Sie die Systemeinstellungen.
9. Wählen Sie im Fenster des **Migrationsassistenten**, dass die Daten **Von einem Mac, Time Machine-Backup oder Startvolume** übertragen werden sollen.
10. Wählen Sie im Fenster **Informationen auf diesen Mac übertragen** das geklonte Laufwerk aus.
11. Wählen Sie im Fenster **Wähle aus, welche Informationen übertragen werden sollen** alle angezeigten Informationen aus und erstellen Sie ein Kennwort.
12. Installieren Sie Acronis Cyber Protect Home Office auf Ihrem Mac.

Sollte die Klonen-Aktion aus irgendeinem Grund gestoppt werden, müssen Sie die Prozedur erneut konfigurieren und starten. Sie werden keine Daten verlieren, weil Acronis Cyber Protect Home Office das ursprüngliche Laufwerk und darauf gespeicherte Daten während des Klonens nicht verändert.

## Ein Fusion Drive klonen

Ein **Fusion Drive** ist ein Hybrid-Laufwerk, bei dem eine relativ langsame HDD (klassische Festplatte) mit einer schnellen SSD (Solid State Drive) kombiniert wird. Ein Fusion Drive wird auf Ihrem Mac wie ein Laufwerk dargestellt, weil der Speicherplatz der beiden Laufwerken zu einem logischen Volume kombiniert wird.

Mit Acronis Cyber Protect Home Office können Sie ein Fusion Drive zu einem anderen Fusion Drive oder zu einem beliebigen anderen Ziellaufwerk klonen.

***So können Sie ein Fusion Drive klonen***

1. Wenn auf Ihrem Mac virtuelle Maschinen (VMs) von Parallels Desktop laufen, sollten Sie sicherstellen, dass diese heruntergefahren sind.
2. Überprüfen Sie, dass die Quell- und Ziellaufwerke an Ihrem Mac angeschlossen sind. Trennen Sie die Verbindung mit allen nicht benötigten externen Laufwerken.
3. Öffnen Sie Acronis Cyber Protect Home Office.

4. Klicken Sie in der Seitenleiste auf **Laufwerk klonen** und dann auf **Fortsetzen**.
5. Wählen Sie ein Fusion Drive als Quelle für die Klonen-Aktion.
6. Schließen Sie das Ziellaufwerk an.
7. Klicken Sie auf das Symbol für das Ziellaufwerk und wählen Sie dann dasjenige Laufwerk aus, welches als Ziel für die zu klonenden Daten fungieren soll.
   Wenn Sie mehr als ein Laufwerk haben, erscheint das Kontrollkästchen **Ein Fusion Drive erstellen**[1]. Wählen Sie dieses aus, wenn Sie ein Fusion Drive erstellen wollen, und wählen Sie dann zwei Laufwerke aus. Bestätigen Sie Ihre Wahl.

   **Warnung!**
   Wenn Sie die Klonen-Aktion starten, wird das Ziellaufwerk formatiert, sodass alle darauf gespeicherten Daten unwiderruflich gelöscht werden. Überprüfen Sie, dass die betreffenden Laufwerke leer sind oder zumindest keine wertvollen Daten enthalten.
8. Klicken Sie auf **Klonen**.

# Zwei Macs verbinden

Wenn Sie Ihre Festplatte zu einem anderen Mac klonen wollen, muss der als Ziel dienende Mac im Festplattenmodus verbunden sein.

***So können Sie den Ziel-Mac mit dem Quell-Mac verbinden***

1. Schalten Sie die als Ziel und Quelle fungierenden Macs ein.
2. Verbinden Sie diese mit einem FireWire- oder Thunderbolt-Kabel.
3. Klicken Sie auf dem Ziel-Mac folgende Befehle an: **Apple-Menü** –> **Systemeinstellungen** -> **Startvolume** – und klicken Sie dann **Festplattenmodus**.
   Nach dem Neustart des Computers erscheint auf dem Desktop des Quell-Macs ein neues Laufwerkssymbol. Ab jetzt können Sie mit der Festplatte des Ziel-Macs wie mit einem gewöhnlichen externen Laufwerk arbeiten – was auch einschließt, dass Sie es als Ziellaufwerk für eine Klonen-Aktion verwenden.
4. Wenn die Klonen-Aktion abgeschlossen wurde, können Sie das Ziellaufwerk auswerfen, indem Sie dessen Symbol einfach in den Papierkorb ziehen.
5. Schalten Sie den Ziel-Mac aus und trennen Sie dann die Kabelverbindung.

[1] Diese Option ist nicht für Macs mit Apple Silicon-Architektur (mit M1- oder M2-Chip) verfügbar.

# Ein Boot-Medium erstellen

## Ein Acronis Boot-Medium erstellen

Acronis Boot-Medium ist ein Wechsellaufwerk, welches entsprechende Boot-Dateien enthält. Sollte Ihr Mac nicht mehr starten, dann verwenden Sie dieses Laufwerk, um eine Wiederherstellungsumgebung von Acronis zu booten. Stellen Sie anschließend damit Ihren Mac aus einem zuvor erstellten Backup wieder her.

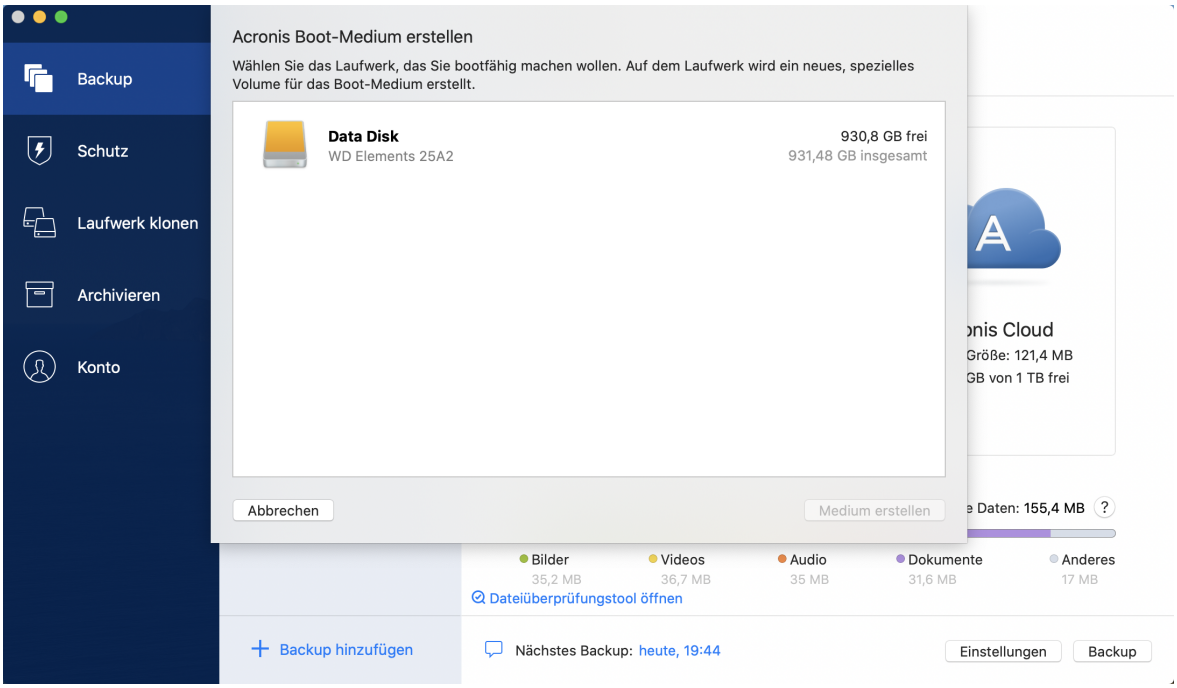
**Hinweis**
Fusion Drives und Laufwerke, die mit SoftRAID initialisiert wurden, werden nicht als Ziele für Acronis Boot-Medium und das Acronis Survival Kit unterstützt.

Sollten Sie bisher noch kein Backup haben, dann erstellen Sie eins. Weitere Details finden Sie im Abschnitt 'Backup zu einem lokalen oder Netzwerk-Storage' bzw. 'Backup in die Acronis Cloud'.

**Warnung!**
Die Verwendung eines Acronis Boot-Mediums ist die einzige Möglichkeit, Ihren Mac aus einem Acronis Cyber Protect Home Office-Backup wiederherzustellen.

***So können Sie ein Acronis Boot-Medium erstellen***

1. Verbinden Sie ein Wechsellaufwerk mit Ihrem Mac.
   Sie können ein Wechsellaufwerk verwenden, welches mit den Dateisystemen APFS oder Mac OS Extended formatiert ist und über 4,3 GB (oder mehr) freien Speicherplatz verfügt. Sie können beispielsweise eine externe Festplatte oder einen USB-Stick verwenden. Beachten Sie, dass CD- und DVD-Medien nicht unterstützt werden.
2. Öffnen Sie Acronis Cyber Protect Home Office.
3. Klicken Sie im Menü **Datei** auf **Acronis Boot-Medium erstellen**. Klicken Sie im dann geöffneten Fenster auf **Medium erstellen**.
4. Das Acronis Media Builder-Fenster wird geöffnet.




5. Wählen Sie das Laufwerk, welches Sie bootfähig machen wollen.
6. Klicken Sie auf den Befehl **Medium erstellen**.

   Acronis Cyber Protect Home Office erstellt ein kleines Volume (Partition) auf dem ausgewählten Laufwerk und speichert in diesem Volume die Boot-Dateien. Um das Volume erstellen zu können, muss eines der bereits vorhandenen Volumes verkleinert werden. Wenn es sich nicht um ein GPT-Laufwerk handelt und es sich bei dem vorhandenen Dateisystem nicht um Mac OS Extended oder APFS handelt, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, das Laufwerk zu formatieren. Beachten Sie dabei, dass durch das Formatieren des Laufwerks auch alle eventuell darauf gespeicherten Daten gelöscht werden.
7. Entfernen Sie das Medium nach Abschluss des Prozesses und bewahren Sie es an einem sicheren Platz auf. Sie können auch eigene Daten auf dem Medium speichern – stellen Sie dabei jedoch sicher, dass Sie keine der Boot-Dateien von Acronis löschen oder ändern.

**Hinweis**

Wir empfehlen, dass Sie jedes Mal ein neues Boot-Medium erstellen, wenn Sie ein Upgrade Ihres macOS auf eine neuere Version durchführen. Anderenfalls funktioniert Ihr Boot-Medium möglicherweise nicht richtig.

**Wichtig**

Wenn Sie ein Mac mit Apple Silicon-Architektur (mit M1- oder M2-Chip) mit einem Acronis Boot-Medium booten, sind Laufwerke, die mit SoftRAID initialisiert wurden, nicht verfügbar.

# Ein Acronis Survival Kit erstellen

## Was ist ein Acronis Survival Kit?

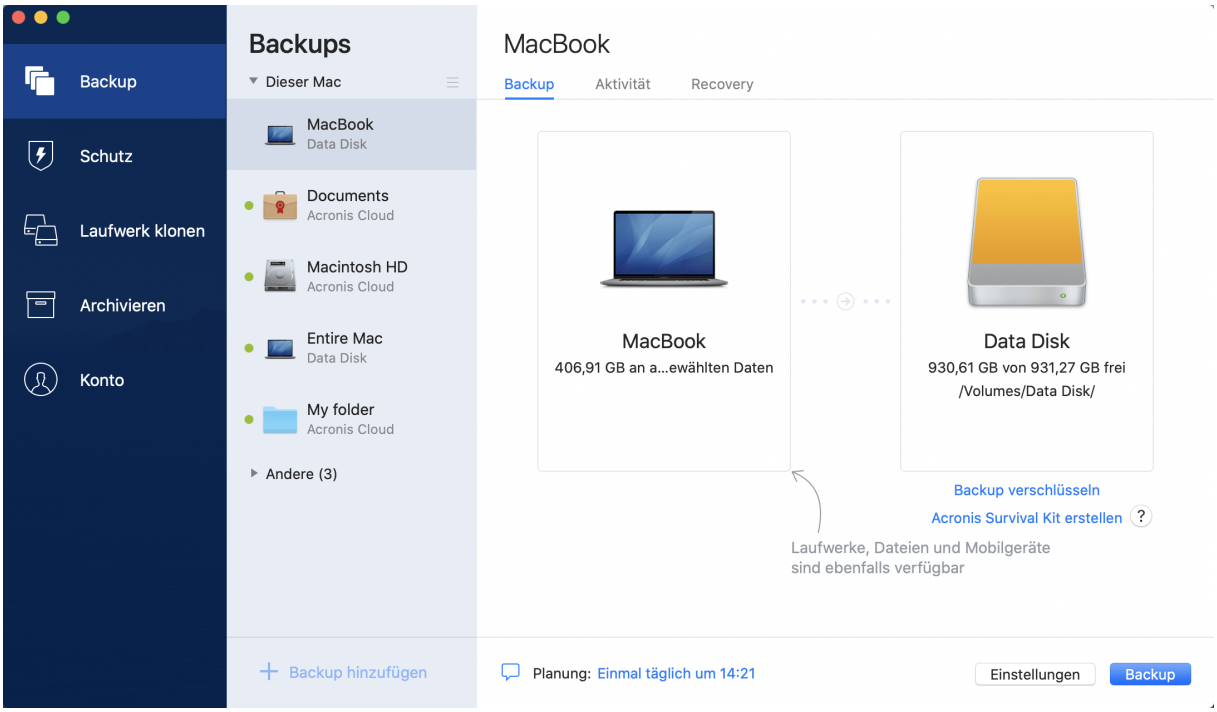
Um Ihren Mac bei einem Ausfall zuverlässig wiederherstellen zu können, benötigen Sie zwei wichtige Komponenten – ein Backup Ihres Systemlaufwerks und ein Boot-Medium. Meistens liegen diese Komponenten getrennt vor – beispielsweise, weil das System-Backup auf einem externen Laufwerk oder in der Acronis Cloud Cloud vorliegt und ein kleiner USB-Stick als Boot-Medium dient. Ein Acronis Survival Kit kombiniert diese beiden Komponenten, sodass Sie ein einziges Gerät erhalten, welches alles enthält, was Sie zur Wiederherstellung Ihres Computers bei einem Ausfall benötigen. Es handelt sich um ein externes Festplattenlaufwerk, welches die Acronis Boot-Medium-Dateien sowie ein Backup Ihres System-Volumes, Ihres kompletten Computers oder eines anderen Laufwerks enthält.

Sie können für das Acronis Survival Kit eine externe Festplatte verwenden, sofern diese größer als 32 GB ist und über Mac OS Extended oder APFS als Dateisystem verfügt. Wenn das Laufwerk ein anderes Dateisystem hat, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, das Laufwerk zu formatieren.

**Hinweis**
Fusion Drives und Laufwerke, die mit SoftRAID initialisiert wurden, werden nicht als Ziele für Acronis Boot-Medium und das Acronis Survival Kit unterstützt.

## Wie kann ich ein Acronis Survival Kit erstellen?

Wenn Sie ein lokales Backup Ihres Systems oder Ihres kompletten Macs konfigurieren und dabei ein externes Festplattenlaufwerk als Ziel auswählen, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, dieses Laufwerk bootfähig zu machen.




***So können Sie ein Acronis Survival Kit erstellen***

1. Klicken Sie auf **Backup jetzt** oder **Acronis Survival Kit erstellen**.
2. Klicken Sie im dann geöffneten Fenster auf **Erstellen**.

   Acronis Cyber Protect Home Office erstellt ein kleines Volume (Partition) auf dem ausgewählten Laufwerk und speichert in diesem Volume die Boot-Dateien. Um das Volume erstellen zu können, muss eines der bereits vorhandenen Volumes verkleinert werden. Wenn es sich nicht um ein GPT-Laufwerk handelt und es sich bei dem vorhandenen Dateisystem nicht um Mac OS Extended oder APFS handelt, wird Ihnen Acronis Cyber Protect Home Office vorschlagen, das Laufwerk zu formatieren. Beachten Sie dabei, dass durch das Formatieren des Laufwerks auch alle darauf gespeicherten Daten gelöscht werden.
3. Wenn die Boot-Dateien erfolgreich auf das Laufwerk geschrieben wurden, ist das Volume zu einem Boot-Medium geworden, welches Sie zur Wiederherstellung Ihres Macs verwenden können. Um die Erstellung des Acronis Survival Kits abzuschließen, müssen Sie noch ein Backup Ihres Systems auf der Festplatte speichern. Klicken Sie dafür auf **Backup jetzt**. Sie können diesen Schritt überspringen, müssen dann aber daran denken, noch später ein entsprechendes System-Backup auf dem Laufwerk zu speichern. Weitere Details finden Sie im Abschnitt 'Backup zu einem lokalen oder Netzwerk-Storage'.

   Wenn Ihr Acronis Survival Kit fertiggestellt ist, können Sie es zur Wiederherstellung Ihres Macs verwenden. Weitere Informationen finden Sie im Abschnitt 'Ihren Mac wiederherstellen'.

# Online Dashboard und Acronis Cloud

## Was ist das Online Dashboard?

Das Online Dashboard ist eine vereinheitlichte, plattformübergreifende Lösung, mit der Sie den Schutzstatus aller Computer, Smartphones und Tablets überwachen sowie steuern können, die alle zusammen im selben Konto registriert sind. Verwenden Sie das Online Dashboard, um den Schutzstatus der Geräte in Ihrem Konto zu überwachen und zu steuern:

- Die Statuszustände aller Backups auf allen Geräten steuern, die entweder Windows, macOS, iOS oder Android als Betriebssystem verwenden.
- Ein neues Gerät zur Liste hinzufügen.
- Ein beliebiges Backup auf jedem Computer manuell starten.
- Neue Backups jeden Typs (Backup des kompletten Maschine, Datei-Backup, Laufwerk-Backup) auf PCs und Macs erstellen.
- Die Einstellungen von bereits vorhandenen Backups ändern.
- Daten aus jedem in der Acronis Cloud gespeicherten Backup wiederherstellen (inkl. der Backups von PCs, Macs sowie von iOS- und Android-basierten Geräten wie Tablets und Smartphones).
- Einige produktbezogene Probleme lösen.
- Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA). Weitere Informationen finden Sie im Abschnitt '"Zwei-Faktor-Authentifizierung (2FA)" (S. 18)'.
- Überwachen Sie die Sicherheit Ihrer persönlichen Daten im Identity Protection Dashboard. Weitere Informationen finden Sie im Abschnitt '"Identitätsschutz" (S. 66)'.

## Ein neues Gerät hinzufügen

1. Öffnen Sie auf dem Gerät, welches Sie hinzufügen wollen, das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Melden Sie sich mit Ihrem Konto an.
3. Klicken Sie in der Registerkarte **Geräte** auf den Befehl **Gerät hinzufügen**.
4. Laden Sie Acronis Cyber Protect Home Office herunter und installieren Sie es.
5. Starten Sie Acronis Cyber Protect Home Office und melden Sie sich mit demselben Konto an.

## Einen beliebigen Computer sichern

Mit dem webbasierten Online Dashboard können Sie einen beliebigen Computer (PC oder Mac) per Backup sichern, sofern dieser am gemeinsam genutzten Konto angemeldet ist.

Sollte von einem Gerät noch kein Backup erstellt worden sein, dann können Sie das Gerät mit den Standardeinstellungen sichern. Acronis Cyber Protect Home Office wird die kompletten Inhalte des Gerätes sichern (beispielsweise mit einem 'Backup des kompletten PCs') und dabei die Acronis

Cloud als Backup-Ziel verwenden. Diese Standardeinstellungen können nicht mit der Acronis Cloud geändert werden. Sie können diese Einstellungen jedoch ändern, wenn Sie Acronis Cyber Protect Home Office auf dem jeweiligen Gerät starten und dort das gewünschte Backup manuell konfigurieren.

***So können Sie einen beliebigen Computer per Backup sichern***

1. Öffnen Sie das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Melden Sie sich mit Ihrem Konto an.
3. Suchen Sie in der Registerkarte **Geräte** dasjenige Gerät, dessen Daten Sie per Backup sichern wollen. Sollte das Gerät offline sein, dann überprüfen Sie, dass es eingeschaltet und mit dem Internet verbunden ist.
4. Gehen Sie folgendermaßen vor:
   - Falls das Gerät schon einmal gesichert wurde, klicken Sie auf **Backup jetzt**.
     Acronis Cyber Protect Home Office erstellt dann – in Übereinstimmung mit dem bereits konfigurierten Backup-Schema – eine neue Backup-Version.
   - Sollte bisher von dem Gerät noch kein Backup erstellt worden sein, dann klicken Sie auf **Backup aktivieren**. Warten Sie anschließend, bis das Backup automatisch konfiguriert wurde und klicken Sie abschließend auf **Backup jetzt**.
     Acronis Cyber Protect Home Office erstellt daraufhin ein neues Voll-Backup und lädt dieses in die Acronis Cloud hoch.

# Daten über das Online Dashboard wiederherstellen

Mit dem webbasierten Online Dashboard können Sie Daten aus jedem Online Backup wiederherstellen, welches von einem Ihrer Geräte (egal ob PCs, Macs, Smartphones oder Tablets) in die Cloud hochgeladen wurde.

***So können Sie Daten aus einem Online Backup wiederherstellen***

1. Öffnen Sie das Online Dashboard über die Adresse: https://cloud.acronis.com.
2. Melden Sie sich mit Ihrem Konto an.
3. Suchen Sie in der Registerkarte **Geräte** dasjenige Gerät, das als 'Recovery-Quelle' dienen soll (von dem aus also die gewünschten Daten wiederhergestellt werden sollen). Sollte das Gerät offline sein, dann überprüfen Sie, dass es eingeschaltet und mit dem Internet verbunden ist.
4. Klicken Sie auf **Recovery**.
5. Wählen Sie im linken Fensterbereich das gewünschte Backup anhand des jeweiligen Backup-Zeitpunkts aus.
6. Aktivieren Sie im rechten Fensterbereich die Kontrollkästchen direkt neben den Dateien bzw. Ordnern, die Sie wiederherstellen wollen.
7. Klicken Sie auf **Download**.

# Was ist Acronis Cloud?

Die Acronis Cloud ist ein geschützter Remote-Storage, den Sie zur Sicherung Ihrer Backups und Archive verwenden können. Da die Dateien auf einem Remote-Storage vorliegen, können Sie die kompletten Inhalte Ihres Macs auch dann wiederherstellen, wenn es zu einem größeren Desaster oder einer Datenbeschädigung kommen sollte.

Sollten Sie Acronis Cyber Protect Home Office für Windows verwenden, dann können Sie außerdem Datei-Backups, Laufwerk-Images sowie Versionen von synchronisierten Dateien in der Acronis Cloud speichern.

***So können Sie mit der Nutzung der Acronis Cloud beginnen***

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Erstellen Sie ein Acronis Konto, falls Sie bisher noch keines haben.
3. [optional] Wenn die Acronis Cloud noch nicht zu Ihrem Abonnement gehört, können Sie sie folgendermaßen aktivieren: klicken Sie in der linken Seitenleiste auf **Konto**. Klicken Sie dann auf **Acronis Cloud aktivieren**. Klicken Sie bei **Acronis Cloud Storage** auf den Befehl **Jetzt testen** oder **Kaufen**.

Die Acronis Cloud-Website ermöglicht Ihnen, die Daten, die Sie in der Acronis Cloud speichern, wiederherzustellen und zu verwalten. Wenn Sie auf die Website zugreifen wollen, gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Konto an. .

## Ein Acronis Konto erstellen

Um den Acronis Cloud Service nutzen zu können, benötigen Sie ein Acronis Konto.

***So können Sie ein Acronis Konto erstellen***

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Wählen Sie 'Acronis Cloud' als Ziel für Ihr Backup. Das Anmeldefenster öffnet sich.
3. Klicken Sie auf **Konto erstellen**.
4. Füllen Sie das Registrierungsformular aus. Geben Sie die erforderlichen Daten ein, akzeptieren Sie die Nutzungsbedingungen und melden Sie sich optional an, wenn Sie gelegentlich News und Werbeangebote erhalten wollen.

   **Hinweis**
   Damit Ihre persönlichen Daten geschützt sind, sollten Sie ein sicheres Kennwort für Ihr Konto festlegen. Sorgen Sie dafür, dass es nicht in falsche Hände gerät – und ändern Sie es von Zeit zu Zeit.

5. Klicken Sie auf **Konto erstellen**.
6. Es wird eine Nachricht an die von Ihnen spezifizierte E-Mail-Adresse gesendet. Öffnen Sie diese Nachricht und bestätigen Sie Ihren Wunsch, ein Konto zu erstellen.

## Abonnement für Acronis Cloud

Einige Funktionen von Acronis Cyber Protect Home Office (wie Online Backup, Cloud-Archivierung und Cloud-Synchronisierung) verwenden die Acronis Cloud und benötigen daher ein Abonnement für den Acronis Cloud Storage. Wenn Sie ein Abonnement abschließen wollen, können Sie Acronis Cyber Protect Home Office öffnen, in der linken Seitenleiste auf **Konto** klicken und dann das gewünschte Abonnement auswählen.

**Hinweis**
Beachten Sie, dass die Nutzung der Acronis Cloud über unsere Richtlinie zur fairen Nutzung (Fair Usage Policy) geregelt wird. Weitere Informationen finden Sie unter https://kb.acronis.com/ati/fairusage.

***Testversion***

Wenn Sie die Testversion des Produktes aktivieren, wird Ihrem Konto automatisch ein kostenloses Acronis Cloud-Abonnement inkl. 1000 GB Cloud-Speicherplatz für die Dauer Ihres Acronis Cyber Protect Home Office-Testzeitraums zugewiesen. Nach Ablauf des Testabonnements funktioniert die Acronis Cloud noch für 30 Tage im Modus 'Nur Recovery'. Nach Ablauf dieses Zeitraums können Sie den Acronis Cloud Service nicht mehr verwenden und Ihre Daten werden komplett aus der Cloud gelöscht.

***So können Sie ein vollständiges Acronis Cloud Storage-Abonnement erwerben***

1. Öffnen Sie Acronis Cyber Protect Home Office.
2. Klicken Sie in der Seitenleiste auf **Konto**. Klicken Sie anschließend auf **Jetzt kaufen**.
3. Wählen Sie das gewünschte Abonnement aus und klicken Sie dann auf **Jetzt kaufen**.
4. Befolgen Sie die Bildschirmanweisungen, um die Kaufvorgang abzuschließen.

Sie können das vollständige Abonnement auch auf der Acronis Website kaufen.

# Lokale Backups in die Acronis Cloud replizieren

## Warum sollten Sie ein Backup replizieren?

Ein Backup alleine bietet zwar einen gewissen, aber nicht umfassenden Schutz für Ihre Daten. Daher empfehlen wir, dass Sie alle lokalen Backups zusätzlich in die Acronis Cloud Cloud replizieren, denn so können Sie Ihren Computer noch besser vor Beschädigungen wie zufälligen Desastern schützen. Sie könnten dafür natürlich einfach zwei Backup-Pläne erstellen – einen zur lokalen Sicherung Ihres Computers und einen zur Sicherung in die Acronis Cloud. Mit einer automatischen Replikation sparen Sie jedoch einerseits Zeit bei der Einrichtung von Backup-Plänen und andererseits ist eine Replikation grundsätzlich schneller als die Erstellung eines weiteren Backups. Ein Replikat ist prinzipiell einfach nur eine zusätzliche, identische Kopie Ihres Backups. Diese bietet einen erweiteren Schutz und kann zudem verwendet werden, um von überall auf Ihre Daten zuzugreifen.

## Eine Replikation aktivieren

Die Replikationsoption ist standardmäßig deaktiviert. Sie können die Replikation für jedes Backup eines Laufwerks, Volumes oder kompletten PCs aktivieren, sofern Sie ein lokales Speicherlaufwerk (z.B. eine externe oder interne Festplatte) als Backup-Ziel und Acronis True Image (2020 oder 2021) oder Acronis Cyber Protect Home Office zur Backup-Konfiguration verwenden. Sie können die Replikation über eine spezielle Registerkarte in einem Backup-Plan aktivieren.

***So können Sie die Replikation eines Backups in die Acronis Cloud aktivieren***

1. Wählen Sie in der Backup-Liste dasjenige Backup aus, das Sie replizieren möchten, und öffnen Sie dann die Registerkarte **Replikat**.
2. Klicken Sie auf **Replizieren**. Jetzt ist die Replikation aktiviert und wird automatisch ausgeführt, sobald das zugrundeliegende Backup erstellt wird. Sie können das Applikationsfenster von Acronis Cyber Protect Home Office jetzt nach Belieben schließen. Das Backup und Replikation werden weiter als Hintergrundprozesse ausgeführt.
3. [Optionaler Schritt] Öffnen Sie die Registerkarte **Backup**, klicken Sie erst auf **Einstellungen** und dann auf **Replikation**, wenn Sie Bereinigungseinstellungen für die Acronis Cloud konfigurieren wollen, um Ihre Speicherplatznutzung zu optimieren.

# Speicherplatz in der Acronis Cloud bereinigen

1. Wenn Sie zur Acronis Cloud gehen wollen, klicken Sie zuerst in der Seitenleiste von Acronis Cyber Protect Home Office auf **Konto** und dann auf den Befehl **Meine Daten durchsuchen**. Die Acronis Cloud-Webseite wird einem Browser geöffnet.
2. Klicken Sie auf der Acronis Cloud-Webseite in der linken Seitenleiste auf **Konto**.
3. Klicken Sie in der Zeile der Acronis Cloud auf den Befehl **Bereinigen**.
4. Wählen Sie, welche Versionen Sie löschen möchten:
   - Versionen, die älter als ein bestimmter Zeitraum sind.
   - Alle alten Versionen, außer einigen neuen.

**Warnung!**
Achtung! Gelöschte Versionen können nicht wiederhergestellt werden.

Eine weitere Möglichkeit zur Bereinigung besteht darin, dass Sie ein nicht mehr benötigtes Cloud Backup löschen. In diesem Fall wird der komplette Versionsverlauf des betreffenden Backups aus der Acronis Cloud gelöscht.

**Siehe auch**

"Backups, Backup-Versionen und Replikate bereinigen" (S. 38)

# Acronis Cloud Backup Download

Acronis Cloud Backup Download ist ein Tool, mit dem Sie Cloud Backups sicher herunterladen können – und das selbst dann, wenn die Internetverbindung instabil ist. Der Download wird nicht mitten drin einfach abgebrochen, wenn die Verbindung ausfallen sollten, sondern er wird nur pausiert und kann später wieder fortgesetzt werden. Außerdem ist eine Wiederherstellung aus einem heruntergeladenen Backup wesentlich schneller als eine Wiederherstellung aus der Cloud.

***So können Sie Acronis Cloud Backup Download installieren***

1. Sie können das Tool auf eine der folgenden Arten herunterladen:
   - Mithilfe von Acronis Cyber Protect Home Office: Klicken Sie im Hauptmenü auf **Datei** –> **Cloud Backups herunterladen**.
   - Gehen Sie zu https://www.acronis.com/my/online-backup/webrestore/ und melden Sie sich an Ihrem Acronis Konto an. Klicken Sie in der Seitenleiste auf **Backups** und wählen Sie dann das Backup aus, dessen Dateien Sie wiederherstellen wollen. Klicken Sie in der Detailansicht auf **Download**. Klicken Sie anschließend im Fenster **Cloud Backups herunterladen** auf **Das Tool herunterladen**. Wählen Sie dann die gewünschte Version des Tools und laden Sie dieses herunter.
   - Gehen Sie zur Download-Seite unter https://go.acronis.com/cloud-backup-download. Wählen Sie dann die gewünschte Version des Tools und laden Sie dieses herunter.

   **Hinweis**
   Das Tool wird auch heruntergeladen, wenn Sie es bereits zuvor installiert haben sollten.
2. Klicken Sie doppelt auf die .dmg-Datei, um diese zu öffnen. Klicken Sie anschließend auf **Acronis Cloud Backup Download**, um das Tool zu starten.
3. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich an.

***So können Sie ein Cloud Backup herunterladen***

**Wichtig**
Sie können nur Backups von Laufwerken, Volumes oder der kompletten Maschine im TIBX-Format herunterladen. Datei- oder Ordner-Backups können nicht mit Acronis Cloud Backup Download heruntergeladen werden.

1. Starten Sie Acronis Cloud Backup Download und melden Sie sich an.
2. Wählen Sie im Fenster '**Acronis Cloud Backup Download**' das Backup aus, das Sie herunterladen wollen.
3. Wählen Sie im Fenster **Backup zum Download auswählen** entweder das gewünschte einzelne Backup oder das komplette Backup-Set aus.
4. [Optionaler Schritt] Wenn das Backup verschlüsselt ist, müssen Sie das entsprechende Kennwort

eingeben.

5. Wählen Sie das Download-Ziel aus und klicken Sie dann auf **Speichern**.

   Der Download der .tibx-Datei wird gestartet. Sie können ihn jederzeit pausieren oder bei Bedarf auch abbrechen.

   ***So können Sie das heruntergeladene Backup verwenden***

   - Wenn Sie die Sicherung der entsprechenden Daten fortsetzen wollen, fügen Sie das Backup zu Acronis Cyber Protect Home Office hinzu (wie im Abschnitt '"Ein vorhandenes Backup der Liste hinzufügen" (S. 40)' beschrieben).
   - Stellen Sie die Daten aus dem Backup wieder her, wie im Abschnitt '"Ihre Dateien und Verzeichnisse wiederherstellen" (S. 57)' beschrieben.
   - Erstellen Sie ein Acronis Survival Kit, wie im Abschnitt '"Ein Acronis Survival Kit erstellen" (S. 77)' beschrieben..
   - Erstellen Sie ein Boot-Medium wie im Abschnitt '"Ein Acronis Boot-Medium erstellen" (S. 75)' beschrieben.

# Daten archivieren

## Was tut die Datenarchivierungsfunktion?

**Hinweis**
Bestimmte Programmfunktionen sind in der von Ihnen verwendeten Edition möglicherweise nicht verfügbar.

Bei der Datenarchivierungsfunktion handelt es sich um ein Tool, mit dem Sie bestimmte Daten (z.B. große oder selten verwendete) auf ein NAS-Gerät, eine externe Festplatte oder einen USB-Stick verschieben können. Sie können die Dateien auch in die Acronis Cloud verschieben. Das Tool analysiert bei jeder Ausführung die Daten im ausgewählten Ordner und schlägt anschließend vor, die gefundenen Dateien zu verschieben. Sie können die Dateien und Ordner auswählen, die Sie archivieren wollen. Nach dem Verschieben in ein Archiv werden die lokalen Kopien dieser Dateien dann gelöscht. Die Links zu diesen Dateien werden an einen speziellen Speicherort mit der Bezeichnung 'Acronis Drive' gespeichert. Sie können auf diesen Speicherort wie auf einen herkömmlichen Ordner im Finder zugreifen. Wenn Sie doppelt auf einen Datei-Link klicken, wird die Datei genauso geöffnet, als wäre in einem lokalen Ordner gespeichert. Sollte die Datei in die Acronis Cloud archiviert worden sein, so wird Sie zuerst wieder auf Ihren Computer heruntergeladen. Die Datei ist zudem auch direkt in der Acronis Cloud verfügbar und verwaltbar.

Die wichtigsten Fähigkeiten bzw. Möglichkeiten der Datenarchivierung sind:

- **Mehr freier Speicherplatz**
  Normalerweise wird der Speicherplatz auf modernen, großen Festplatten überwiegend durch Benutzerdaten (Fotos, Dokumente etc.) belegt – und nicht so sehr durch das Betriebssystem oder Software-Anwendungen. Da die Mehrzahl dieser Benutzerdaten nur selten verwendet wird, ist es nicht zwingend notwendig, diese auch ständig auf einem lokalen Laufwerk vorzuhalten. Die Datenarchivierungsfunktion hilft Ihnen, mehr Speicherplatz freizugeben, sodass dieser besser für häufig verwendete Dateien genutzt werden kann.
- **Cloud-Archivierung und lokale Archivierung**
  Sie können einen Zieltyp für Ihr Archiv bestimmen: eine interne oder externe Festplatte, ein NAS-Gerät oder einen USB-Stick. Sie können außerdem auch die Acronis Cloud wählen. Wenn Sie die Acronis Cloud als Ziel auswählen, werden die ausgewählten Daten immer in demselben Cloud-Archiv gespeichert. Lokale Archive sind unabhängig von einander und können daher (bei Bedarf) unterschiedliche Namen, Zielorte, Verschlüsselungseinstellungen usw. haben. Sie können jedoch auch hier immer ein vorhandenes Archiv als Ziel auswählen (statt ein neues zu erstellen). Die Anzahl der lokalen Archive ist nicht begrenzt.
- **Einfacher Zugriff auf Cloud-Archive von beliebigen Geräten**
  Wenn Sie Ihre Dateien in die Acronis Cloud archiviert haben, können Sie auf diese anschließend leicht über Acronis Cyber Protect Home Office, über die Acronis Cyber Protect Home Office Mobile App (für Mobilgeräte) und direkt über die Webseite der Acronis Cloud zugreifen. Also mit

allen Geräten (einschließlich Smartphones und Tablets), auf denen entweder Windows, macOS, iOS oder Android als Betriebssystem läuft.

- **Schutz Ihrer Daten im Cloud-Archiv**

  Ihre in der Acronis Cloud gespeicherten Daten sind zuverlässig vor Beschädigungen oder einem Desaster (etwa ein Feuer, Wasserschaden oder Einbruch in Ihrer Wohnung) geschützt. Sollte beispielsweise Ihre lokale Festplatte kaputtgehen, können Sie Ihre Dateien ganz einfach auf eine neue Festplatte herunterladen. Ihre Daten werden zudem verschlüsselt gespeichert. Daher haben Sie die Gewissheit, dass nur Sie (und sonst wirklich niemand, auch nicht Acronis) auf Ihre Daten zugreifen kann.
- **File-Sharing**

  Sobald Ihre Dateien in die Acronis Cloud hochgeladen wurden, können Sie öffentliche Links auf diese erstellen. Mit diesen Links können Sie die Dateien für bestimmte Personen (z.B. Freunde) oder in Foren und sozialen Netzwerken freigeben.
- **Dateiversionen**

  Bei Dateien, die geändert und dann entsprechend mehrfach in die Acronis Cloud hochgeladen werden, speichert Acronis Cyber Protect Home Office all diese durchgeführten Änderungen in Form von einzelnen Dateiversionen. Sie können daher jederzeit eine bestimmte, gewünschte Dateiversion auswählen und wieder auf Ihr Gerät herunterladen.

## Was wird von Archiven ausgeschlossen?

Standardmäßig werden von Acronis Cyber Protect Home Office folgende Daten/Dateien von den Archiven ausgeschlossen, um die Archivgröße zu senken und Risiken zur Beschädigung Ihres Systems zu vermeiden:

- pagefile.sys
- swapfile.sys
- Der Ordner für den Netzwerk-Papierkorb
- Der Ordner 'System Volume Information'
- Der 'Papierkorb'
- .tib- und .tibx-Dateien
- .tib.metadata-Dateien
- .tmp-Dateien
- Dateien mit der Erweiterung .~

Eine vollständige Dateiliste finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/de/content/58297.

# Cloud-Archivierung vs. Online Backup

Wenn Sie Daten in die Acronis Cloud archivieren, gleicht dies zwar einem Online Backup, aber es gibt auch einige Unterschiede.

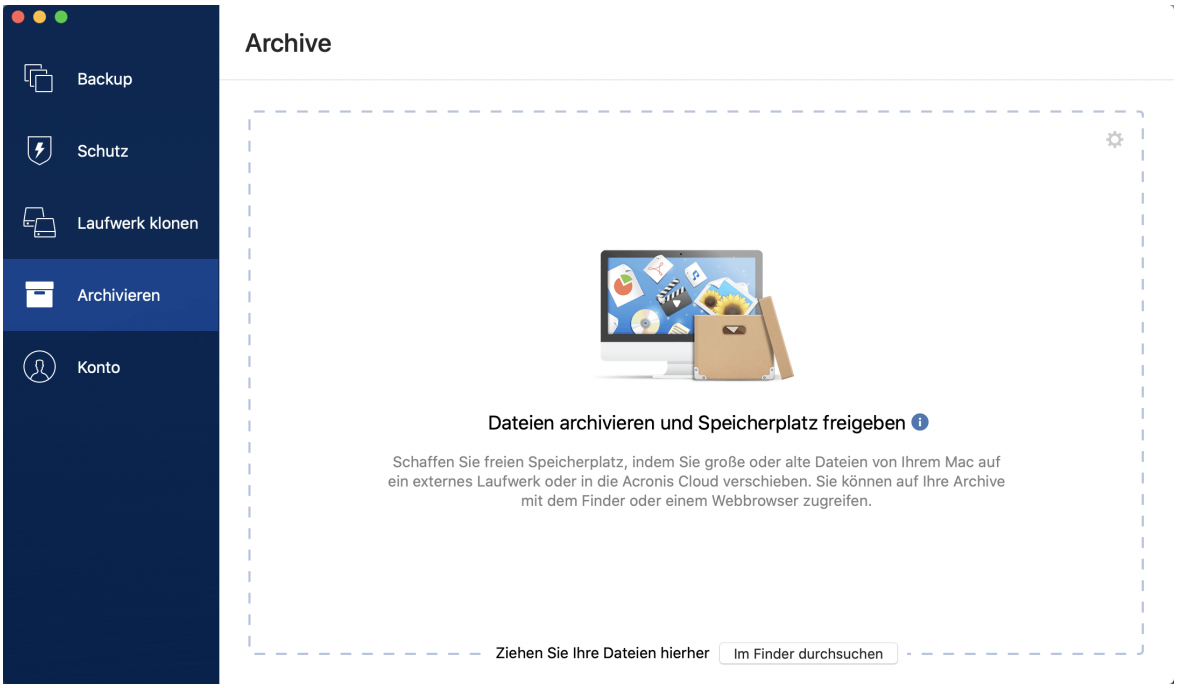
| | Online Backup | Cloud-Archivierung |
|---|---|---|
| Verwendungszweck | Schutz vor Beschädigung des Betriebssystems, Hardware-Fehlern und Verlust einzelner Dateien. | Bereinigung lokaler Speichergeräte und Datenverschiebung in die Acronis Cloud. |
| Data Protection | • Umfassende Sicherung all Ihrer Daten auf einem Computer (insbesondere des Betriebssystems).<br>• Sicherung von häufig verwendeten Dateien. | Sicherung von selten verwendeten oder alten Dateien (v.a. persönliche Dokumente, Fotos etc.). |
| Auswahl der Quelldaten | Manuelle Auswahl. | Manuelle Auswahl. |
| Handhabung der Quelldaten | Die Quelldaten bleiben am ursprünglichen Speicherort. | Die Quelldaten werden vom ursprünglichen Speicherort gelöscht. Dadurch erhalten Sie die Garantie, dass Ihre Daten nicht in falsche Hände geraten können (z.B. falls Ihr Computer oder Ihre Festplatte gestohlen werden sollten). |
| Häufigkeit von Datenänderungen | Die zu sichernden Daten werden häufig geändert. Zum Backup gehören viele, immer wieder aktualisierte Versionen. | Die zu archivierenden Daten werden selten geändert. Zu dieser Datei gibt es nur wenige Versionen. |

# Archivierung Ihrer Daten

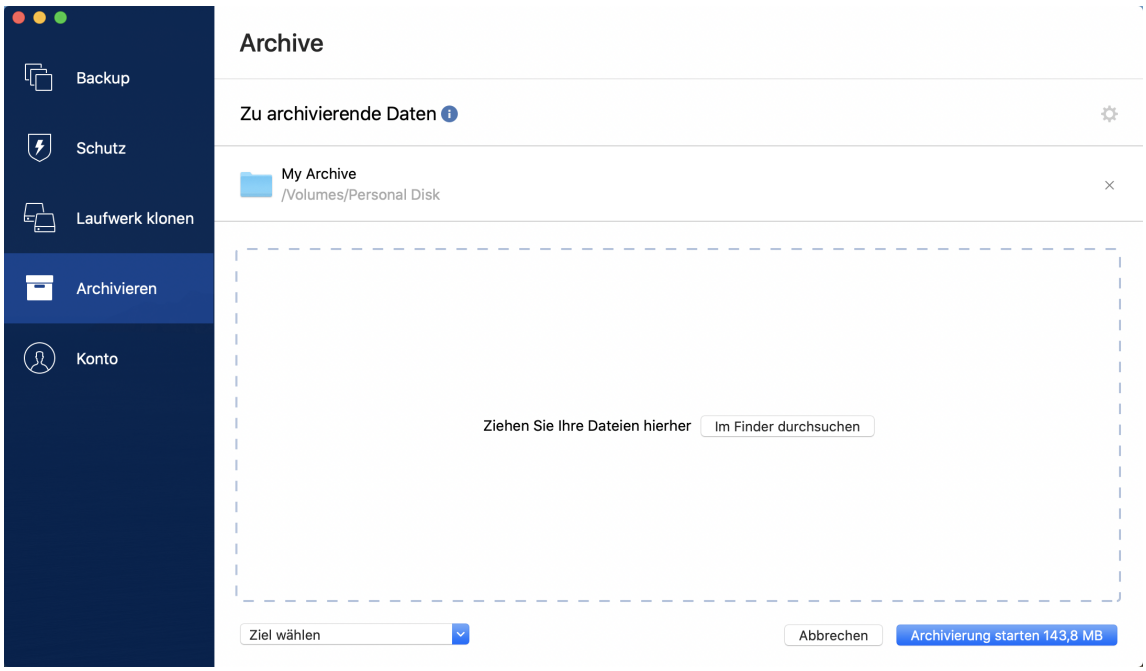
Die Datenarchivierungsfunktion hilft Ihnen, lokalen Speicherplatz freizugeben, indem Sie alte oder selten verwendete Dateien zu einem anderen Storage verschieben. Weitere Informationen finden Sie im Abschnitt 'Was tut die Datenarchivierungsfunktion'.

***So können Sie Ihre Daten archivieren***

1. Starten Sie Acronis Cyber Protect Home Office und wechseln Sie in den Programmbereich **Archivieren**.




2. [Optionaler Schritt] Wenn Sie die Grundlagen der Datenarchivierungsfunktion lernen wollen, schauen Sie sich die 'Erste Schritte'-Folien an.
3. Verwenden Sie eine der nachfolgenden Möglichkeiten, um die zu archivierenden Dateien auszuwählen:
   - Ziehen Sie die Dateien (beispielsweise vom Finder aus) in die Archivierungsanzeige.
   - Klicken Sie auf **Im Finder durchsuchen** und wählen Sie die Dateien aus, die archiviert werden sollen.




4. Klicken Sie auf **Ziel wählen** und wählen Sie dann eine Zielspeicherort für die zu archivierenden Dateien.

5. [Optionaler Schritt] Klicken Sie auf das Zahnradsymbol, wenn Sie noch weitere Einstellungen konfigurieren wollen. Sie können:
   - Ihr Archiv per Kennwort und Verschlüsselung unter **Einstellungen** —> **Verschlüsselung** schützen. Weitere Details finden Sie im Abschnitt 'Archiv-Verschlüsselung'.
   - Wählen Sie das von Ihnen bevorzugte Datacenter und konfigurieren Sie die Upload-Geschwindigkeit (unter **Einstellungen** —> **Erweitert**). Weiter Details finden Sie im Abschnitt 'Acronis Cloud-Datacenter auswählen'.
6. Klicken Sie auf **Archivierung starten**.
7. Bestätigen Sie, dass Sie die Dateien in das Archiv verschieben und automatisch von Ihrem Computer löschen lassen wollen.

# Netzwerkeinstellungen für Archivierungen

## Datacenter

Wenn Sie Ihrer Dateien in die Acronis Cloud archivieren, werden Ihre Daten in eines der Acronis Datacenter hochgeladen, die jeweils in verschiedenen Ländern liegen. Beim Erstellen Ihres Acronis Kontos wird anfänglich dasjenige Datacenter für Sie festgelegt, welches Ihrem Standort am nächsten liegt. Anschließend werden Ihre archivierten Dateien standardmäßig in genau diesem Datacenter gespeichert.

Wir empfehlen, dass Sie dann ein anderes Datacenter für ein Archiv manuell festlegen, wenn Sie sich in einem anderen Land befinden – oder das standardmäßig ausgewählte Datacenter doch nicht das nächstliegende ist (bezogen auf Ihren Stand- bzw. Wohnort). Dies kann die Datenrate beim Upload deutlich steigern.

**Hinweis**
Sie können das Datacenter nicht mehr ändern, nachdem der Archivierungsprozess gestartet wurde.

***So können Sie ein Datacenter auswählen***

1. Klicken Sie beim Konfigurieren des ersten Archivierungsprozesses auf das Symbol für **Einstellungen** und dann auf die Option **Netzwerk**.
2. Wählen Sie dasjenige Land aus, das am nächsten zu Ihrem aktuellen Stand- bzw. Wohnort liegt. Klicken Sie anschließend auf **OK**.

## Upload-Geschwindigkeit

Wenn Sie Daten in die Acronis Cloud archivieren, können Sie festlegen, welche maximale Netzwerkverbindungsgeschwindigkeit Acronis Cyber Protect Home Office dabei verwenden soll. Legen Sie dazu eine Verbindungsgeschwindigkeit fest, bei der Sie das Internet ohne störende Performance-Einbußen (für andere Prozesse) weiternutzen können.

Verwenden Sie eine der folgenden Optionen, um die Verbindungsgeschwindigkeit festzulegen:

- **Maximum** – Die Datenübertragungsrate ist (auf Basis der Grenzen der vorhandenen Systemkonfiguration) maximal.
- **Benutzerdefiniert** – Sie können für die Upload-Geschwindigkeit einen maximalen Wert festlegen.

## Archiv-Verschlüsselung

Um die archivierten Daten gegen unberechtigte Zugriffe zu schützen, können Sie das Archiv mit dem AES-Algorithmus (Advanced Encryption Standard) verschlüsseln lassen, wobei eine Verschlüsselungstiefe von 256 Bit verwendet wird.

**Hinweis**
Die Option zur Archiv-Verschlüsselung kann nicht für bereits vorhandene Archive festgelegt oder geändert werden.

***So können Sie ein Archiv verschlüsseln***

1. Klicken Sie beim Konfigurieren des ersten Archivierungsprozesses auf das Symbol für **Einstellungen** und dann auf die Option **Verschlüsselung**.
2. Geben Sie das Kennwort für das Archiv in das enstprechende Feld ein und klicken Sie dann auf **OK**.

   Wir empfehlen die Verwendung eines Kennworts, das aus mindestens acht Zeichen besteht und sowohl Buchstaben (am besten Groß- und Kleinbuchstaben) wie Zahlen enthält, damit es nicht leicht zu erraten ist.

   Ein Kennwort kann nicht wieder abgerufen werden. Sie sollten Sie das zum Schutz des Archivs vergebene Kennwort daher sehr gut merken.

# Zugriff auf Ihre archivierten Dateien

Wenn Ihre Dateien erfolgreich archiviert sind, können Sie folgendermaßen auf diese zugreifen:

- **Finder**

  Öffnen Sie auf Ihrem Mac den Finder und klicken Sie unter Favoriten auf **Acronis Drive**.

  Die Dateien sind im Backup schreibgeschützt, Sie können mit ihnen im Nur-Lesen-Modus arbeiten (z.B. die Dateien anzeigen). Wenn Sie eine Datei richtig bearbeiten (ändern) wollen, müssen Sie diese zuerst in einen anderen Ordner kopieren.
- **Acronis Cloud** (nur für Cloud-Archive gültig)
  1. Öffnen Sie Acronis Cyber Protect Home Office, klicken Sie auf **Archive** und dann auf **Im Webbrowser öffnen**.
  2. Wählen Sie in der Registerkarte **Archiv** der Acronis Cloud-Website das gewünschte Archive über das Kontrollkästchen aus.
  3. Klicken Sie in der rechten Seitenleiste auf **Download**.
  4. Die ausgewählten Daten werden zum vorgegebenen Download-Ordner kopiert.

# Daten freigeben

Sie können die Daten und Ordner, die in den Backups und Archiven vorliegen, die in der Acronis Cloud gespeichert sind, mit anderen Personen teilen bzw. für diese freigeben.

1. Klicken Sie in der Seitenleiste von Acronis Cyber Protect Home Office auf **Konto**.
2. Klicken Sie im Bereich **Acronis Cloud Storage** auf den Befehl **Meine Daten durchsuchen**. Sie werden zur Acronis Cloud-Webseite weitergeleitet.
3. Gehen Sie folgendermaßen vor, je nachdem, was Sie freigeben wollen:
   - Wenn Sie Dateien oder Ordner aus einem Backup freigeben wollen, klicken Sie in der linken Seitenleiste auf **BACKUPS**. Wählen Sie die gewünschte Datei oder den gewünschten Ordner über das entsprechende Kontrollkästchen aus.
   - Wenn Sie Dateien oder Ordner aus einem Archiv freigeben wollen, klicken Sie in der linken Seitenleiste auf **ARCHIVE**. Wählen Sie die gewünschte Datei oder den gewünschten Ordner über das entsprechende Kontrollkästchen aus.
4. Klicken Sie in der Seitenleiste auf **Link teilen**.
5. [Optional] Sie können Freigabe-Optionen konfigurieren. Klicken Sie dafür im entsprechenden Fenster auf **Link-Einstellungen**. Sie können ein Kennwort zuweisen, ein Ablaufdatum festlegen und die Anzahl der Downloads begrenzen.
6. Klicken Sie im Freigabe-Fenster auf den Befehl **Link kopieren** und schließen Sie das Fenster.

Sie können diesen Link jetzt mit anderen Personen teilen. Wenn Sie die freigegebenen Dateien einsehen wollen, müssen Sie in der linken Seitenleiste auf **FREIGEBEN** klicken. Sie können hier jede Datei auswählen und in der rechten Seitenleiste den entsprechenden Link kopieren, die Linkeinstellungen konfigurieren oder diese löschen.

# Index