Acronis

acronis.com

Acronis Cyber Protect

Home Office

User Guide

REVISION: 8/30/2021

Table of contents

Copyright statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 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; and patent pending applications.

1 Introduction

1.1 What is Acronis Cyber Protect Home Office?

Acronis Cyber Protect Home Office is an application that protects all information on your Mac, including the operating system, applications, settings, and all of your data.

To protect your Mac, you need to perform two easy operations:

1. **Create a complete backup of your Mac.**
   This saves your operating system files and all your data to a file called backup. You can store this file in local or network storage or upload it on Acronis Cloud. Refer to Backing up to local or network storage and Backing up to Acronis Cloud.
2. **Create Acronis bootable media.**
   This is a removable drive containing boot files. When your Mac cannot start up, this media allows you to start an Acronis recovery environment and use your backup to rollback your Mac to a healthy state. Refer to Creating Acronis bootable media for details.

After performing these two steps, you can be sure that you will be able to repair your macOS and recover your lost documents in a few minutes.

Key features:

- Backup of selected disks or entire Mac contents to local or network storage or to Acronis Cloud
- Backup of selected files and folders to local or network storage or to Acronis Cloud
- Antivirus Protection
- Data archiving
- Family data protection
- Creating Acronis bootable media
- macOS recovery in the bootable media environment
- Recovery of specific files and folders under macOS

1.2 System requirements

Supported operating systems

- macOS Big Sur 11
- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

Note
Mac machines with Intel Core 2 Duo processors are not supported.

Supported file systems

- APFS
- HFS+ (including Core Storage)
- FAT32
- NTFS (including Boot Camp)

Note
You cannot back up data to a disk with an NTFS file system. However, you can recover data from a backup located on this type of file system.

Requirements for Acronis bootable media

- To create a bootable media, you can use any removable drive with 4 GB (or more) of free space and that is formatted with the Mac OS Extended file system.
- The version of macOS Recovery must match the version of macOS installed on your Mac.
- CD and DVD media are not supported.

Supported storage media

- Internal drives (HDD, SSD, RAID)
- USB drives
- FireWire drives
- Thunderbolt drives
- Network share, NAS
- Acronis Cloud

Supported processors

- Apple silicon
- Intel (x86)

General requirements

- You need to have administrator privileges to run Acronis Cyber Protect Home Office.
- [On an Intel-based Mac, except Big Sur] If your Mac includes the Apple T2 chip, select "Medium Security" and "Allow booting from external media" in the Secure boot settings. For more information, refer to https://support.apple.com/en-us/HT208330.
- [On an Intel-based Mac, for Big Sur] If your Mac includes the Apple T2 chip, select "No Security" and "Allow booting from external media" in the Secure boot settings. For more information, refer to https://support.apple.com/en-us/HT208330.

Dark Mode support

Dark Mode is available in macOS Mojave or later. Acronis Cyber Protect Home Office switches to the dark appearance when Dark Mode is turned on in macOS.

1.3 Install, update, or remove Acronis Cyber Protect Home Office

To install Acronis Cyber Protect Home Office

1. Download the Acronis Cyber Protect Home Office setup file from the Acronis website at http://go.acronis.com/home-office.
2. Double-click the Acronis Cyber Protect Home Office setup file (the file has a .dmg extension).
3. Double-click **Install Acronis Cyber Protect Home Office** in the **Acronis Cyber Protect Home Office** window.
4. Follow the installer steps. When prompted, provide administrator credentials.
5. Read and accept the terms of the license agreement and the Acronis Customer Experience Program.
6. When you start Acronis Cyber Protect Home Office for the first time, you can do one of the following in the **Activation** window:
   - To activate Acronis Cyber Protect Home Office, enter your serial number, and then click **Activate**. The product will be activated.
   - To sign in to your Acronis account, click **Sign in**. Refer to "Activating Acronis Cyber Protect Home Office" (p. 10) for details.
   - To start trial, click **Start trial**.

On macOS High Sierra 10.13, Mojave 10.14, or Catalina 10.15, you need to grant access to Acronis International GmbH after the installation. It is required for loading kernel extensions in order to have all the protection features. Please do the following:

1. Open **System Preferences**.
2. Go to the **General** tab of **Security & Privacy**.
3. Click **Allow** to accept the prompt that appears.

You also need to grant full disk access to Acronis Cyber Protect Home Office. On macOS Mojave 10.14 or Catalina 10.15, backup, cloning, and protection will not work properly without the full disk access. On macOS Big Sur 11, backup and cloning will not work properly, and protection will be disabled without the full disk access. To grant the access, when the window requesting Full Disk Access appears, follow the on-screen instructions. Refer to https://kb.acronis.com/content/61832 for details.

To update Acronis Cyber Protect Home Office

When an update for Acronis Cyber Protect Home Office is available from the Acronis website, you will be notified. Then you can download it. Then, install it over your version of Acronis Cyber Protect Home Office. All your backups and settings will be kept.

To turn on an automatic check, in the Acronis Cyber Protect Home Office menu, click **Preferences**, and then select the **Automatically check for updates at startup** check box (selected by default).

To check for updates manually, in the Acronis Cyber Protect Home Office menu, click **Check for Updates**.

To remove Acronis Cyber Protect Home Office

1. Download the Acronis Cyber Protect Home Office setup file from the Acronis website.
2. Double-click the Acronis Cyber Protect Home Office setup file (the file has a .dmg extension).
3. Double-click **Uninstall Acronis Cyber Protect Home Office** in the **Acronis Cyber Protect Home Office** window, and confirm uninstalling.
4. When prompted, provide administrator credentials.

1.4 Activating Acronis Cyber Protect Home Office

To use Acronis Cyber Protect Home Office, you need to activate it via the internet. Without activation the fully functional product works for 30 days. If you do not activate it during that period, all the program functions become unavailable except the recovery.

You can activate Acronis Cyber Protect Home Office either on your computer or from another computer, if your computer is not connected to the internet.

Activation on a computer connected to the internet

If your computer is connected to the internet, the product will be activated automatically.

If the computer where you install Acronis Cyber Protect Home Office does not have internet connection or if the program cannot connect to Acronis Activation Server, click **Account** on the sidebar, and then select one of the following actions:

- **Try again** - Select this option to try to connect to the Acronis Activation Server again.
- **Activate offline** - You can activate the program manually from another computer that is connected to the internet (see below).

Activation from another computer

If your computer is not connected to the internet, you may activate Acronis Cyber Protect Home Office by using another computer which has connection to the internet.

To activate the product from another computer

1. On your computer, install and start Acronis Cyber Protect Home Office.
2. On the sidebar, click **Account**, and then click **Activate offline**.
3. In the Acronis Cyber Protect Home Officeactivation window, perform the following simple steps:
   a. Save your installation code to a file by clicking the **Save to file** button, and specify a removable media as the file location (for example, a USB flash drive). You may also simply write down this code on a piece of paper.
   b. On another computer which has an internet connection, go to https://www.acronis.com/activation/. The instructions on the screen will help you to get your activation code by using the installation code. Save the obtained activation code to a file on a removable media, or write it down on paper.

c. On your computer, click the **Load from file** button and specify a path to the file with the activation code; or, simply type it into the box from the piece of paper.

4. Click **Activate**.

Additionally, watch the English-language video instructions at https://goo.gl/DHd1h5.

1.4.1 Too many activations

Possible reasons for the "Too many activations" issue:

- **You exceed the maximum number of computers with installed Acronis Cyber Protect Home Office.**

  For example, you have one license or a serial number for one computer and you install Acronis Cyber Protect Home Office on a second computer.

  Solutions:

  - Enter a new serial number. If you do not have one, you can buy it in the Acronis built-in store or at the Acronis website.
  - Move the license from another computer on which the product is already activated to your new computer. To do this, select the computer from which you want to move the license. Note that Acronis Cyber Protect Home Office will be deactivated on that computer.

- **You reinstall macOS or change hardware in your computer.**

  For example, you might upgrade the motherboard or processor in your computer. Activation will be lost, because Acronis Cyber Protect Home Office sees your altered computer as a new one.

  Solution:

  To reactivate Acronis Cyber Protect Home Office on your computer, choose the same computer identified by its old name from the list.

1.4.2 Managing your subscription licenses manually

If you use the subscription-based version of Acronis Cyber Protect Home Office, you can manage the licenses manually at the Acronis website. You can do the following:

- Move licenses between your computers
- Transfer licenses between your accounts
- Remove a license from a computer
- Resolve product activation conflicts, including the "Too many activations" issue
- Buy new licenses

To manage licenses

1. Go to https://account.acronis.com/, and then sign in with your Acronis account.
2. In the **Products** section, find Acronis Cyber Protect Home Office, and then click **Manage**.

1.5 Trial version information

If you want first to try and evaluate Acronis Cyber Protect Home Office, you can install the free, 30-day trial version of the product. After the trial period, the program functionality is blocked and you will need to upgrade to the full version if you wish to continue using Acronis Cyber Protect Home Office. Note that Disk cloning is disabled in the trial version.

After the trial period expires, your local and network backups are not deleted and can be used for recovery in the full version of Acronis Cyber Protect Home Office.

You have 1000 GB of storage space on the cloud during the trial period. You can use this space to store your online backups. After the trial period is over, Acronis Cloud works in recovery-only mode for 30 days. After this period, you won't be able to use the Acronis Cloud service and all your data will be deleted.

To install the trial version

To start using the trial version, install the product, and then click **Start Trial** in the **Activation** window. Refer to Install, update or remove Acronis Cyber Protect Home Office for details.

To upgrade to the full version of the product

1. Purchase the full version at the Acronis website: https://go.acronis.com/mac/getfullversion.
2. Open Acronis Cyber Protect Home Office.
3. On the Acronis Cyber Protect Home Office menu bar, click **Enter Serial Number**.
4. Insert the full serial number in the appropriate box, and then click **Activate**.

1.6 Acronis Customer Experience Program

Acronis Customer Experience Program (CEP) is a new way to allow Acronis customers to contribute to the features, design and development of Acronis products. This program enables our customers to provide us with various information, including information about the hardware configuration of your host computer and/or virtual machines, the features you use most (and least), and the nature of the problems you face. Based on this information, we will be able to improve the Acronis products and the features you use most often.

To join or leave Acronis Customer Experience Program

1. In the Acronis Cyber Protect Home Office menu, click **Preferences**.
2. To leave the program, clear the **Participate in the Acronis Customer Experience Program** check box.

If you choose to participate, the technical information will be automatically collected every week. We will not collect any personal data, like your name, address, phone number, or keyboard input. Participation in the CEP is voluntary, but the end results are intended to provide software improvements and enhanced functionality to better meet the needs of our customers.

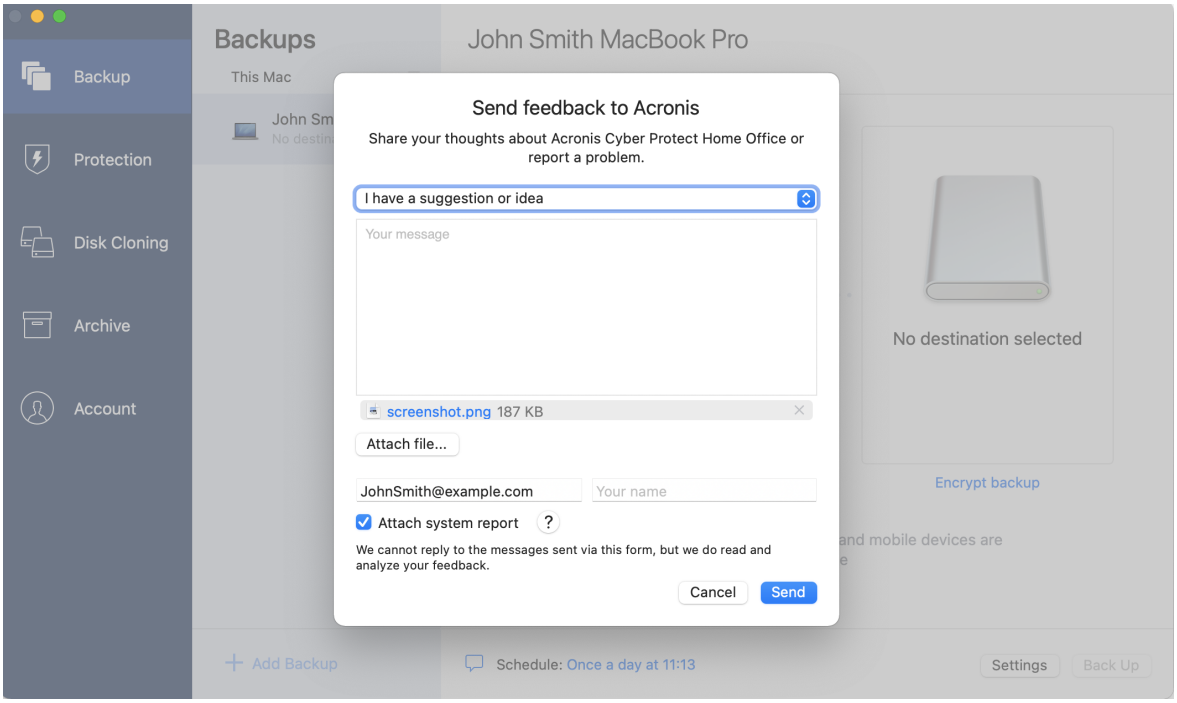
1.7 Sending feedback to Acronis

We frequently improve our products and services by making them more functional, reliable, and fast. Via the feedback form, you can point out inconveniences and defects that we should resolve to make Acronis Cyber Protect Home Office even better. Please spend a couple of minutes to tell us what you think about our product, suggest a new feature, or report a problem. We do read and analyze all feedback.

Note
We do not reply to all feedback messages. If you need assistance with Acronis Cyber Protect Home Office, contact Technical Support.

To send feedback to Acronis

1. In the Acronis Cyber Protect Home Office menu, click **Send feedback**. The feedback form opens.



2. Choose a feedback reason from the list.
3. Type your message.
4. Provide your name and email.
5. [Optional step] By default, Acronis Cyber Protect Home Office attaches a screenshot of the console window. You can delete it if you think it will not help us investigate your issue or understand your idea.
6. [Optional step] You can also attach a file and Acronis system report.

   An Acronis system report contains various technical information, including information about your hardware configuration, macOS version, system log, event log of Acronis Cyber Protect Home Office, and your backup settings.

Note
An Acronis system report does not contain any personal data, like your name, address, phone number, or keyboard input.

We recommend that you attach the system report when you faced a serious error, for example, when Acronis Cyber Protect Home Office stopped responding.

7. Click **Send**.

1.8 Application preferences

The Preferences window contains general settings of Acronis Cyber Protect Home Office. To open it:

1. Open Acronis Cyber Protect Home Office.
2. In the Acronis Cyber Protect Home Office menu, click **Preferences**.

The following settings are available on the **General** tab:

- **Back up when your Mac is in Power Nap**
  The backup may be executed when your Mac is sleeping. Refer to Scheduling for details.
- **Automatically check for updates at startup**
  Refer to Install, update, or remove Acronis Cyber Protect Home Office for details.
- **Participate in the Acronis Customer Experience Program**
  Refer to Acronis Customer Experience Program for details.
- **Show notifications in Notification Center**
  Refer to Notifications for details.
- **Show personalized offers**
  Select this check box to receive personalized offers about products and features.

The following settings are available on the **Battery Saver** tab:

- **Do not back up when working on battery power**
  Refer to Laptop power settings for details.

The following settings are available on the **Wi-Fi Networks** tab:

- **Back up using only selected Wi-Fi networks**
  Refer to Wi-Fi networks for backup to Acronis Cloud for details.

1.9 Keyboard shortcuts

In Acronis Cyber Protect Home Office, you can use the keyboard shortcuts to navigate the user interface in a more comfortable and fast way. To apply a shortcut, press two or more keys of a key combination simultaneously. Some of the Acronis Cyber Protect Home Office shortcuts are specified in the application menu. In menus, some key names are replaced with the following icons:

Key name	Icon
Command	⌘
Option	⌥
Shift	⇧

Keyboard shortcuts in Acronis Cyber Protect Home Office:

Shortcut	Description
Command + U	Check for the product updates
Shift + Command + E	Enter serial number
Command + ,	Open the application preferences window
Shift + Command + L	Sign in to your account
Shift + Command + O	Sign out from your account
Command + N	Create new backup
Command + 1	Open the **Backup** section
Command + 2	Open the **Protection** section
Command + 3	Open the **Disk Cloning** section
Command + 4	Open the **Archive** section
Command + 5	Open the **Account** section
Backup section	
Command + S	Open the backup source dialog
Command + D	Open the backup destination dialog
Command + Shift + S	Open the backup settings dialog
Disk Cloning section	
Command + S	Open the cloning source dialog
Command + D	Open the cloning destination dialog
Archive section	
Command + O	Open the file selection dialog to add files to an archive
Command + D	Open the archive destination dialog
Command + I	Open the archiving tutorial window
Command + Shift + S	Open the archiving settings dialog

1.10 Integration with Touch Bar

Starting from models of 2016, on 15-inch MacBook Pro and 13-inch MacBook Pro with four Thunderbolt 3 ports, there is a special interaction area, called Touch Bar, on the upper part of the keyboard. Touch Bar displays the most appropriate set of controls depending on the currently active window or the task that you are working on at this or that moment. This technology simplifies your interaction with user interface and allows you to perform a wide range of operations, for example, click buttons, switch between websites, use search, change text formatting, and use standard Mac system controls. See more information about Touch Bar at the Apple website: https://support.apple.com/en-us/HT207055.

Acronis Cyber Protect Home Office supports the functionality of Touch Bar. You can use it to switch between different application sections, configure backups, recover data, and other operations. For example when you select a backup from the list, the Touch Bar looks like this:

The **Esc** button and the icons to the right are Mac's system controls. The left part contains icons for navigating between the sections of Acronis Cyber Protect Home Office:

Icon	Description
	Backup
	Disk Cloning
	Archive
	Protection
	Account

The controls that refer to the current window are located in the central part. In this example you can change the backup source, destination, settings (), and start the backup.

You can also create a new backup or archive by using the Touch Bar icons:

Icon	Description
	Create a new backup
	Create a new archive or add files to an existing one

1.11 Technical Support

If you need assistance with your Acronis product, please go to https://www.acronis.com/support/.

You can download the latest updates for all your registered Acronis software products from our website at any time after logging into your **Account** (https://account.acronis.com/) and registering the product. See **Registering Acronis Products at the Website** (https://kb.acronis.com/content/4834) and **Acronis Website User Guide** (https://kb.acronis.com/content/8128).

2 Backup

2.1 Basic concepts

Backup and recovery

Backup refers to making copies of data so that they can be used to **recover** the original data after a data loss event.

Backups are useful primarily for two purposes:

- To recover an operating system when it is corrupted or cannot start. This process is called disaster recovery. For information about protecting your Mac from a disaster, refer to Backing up to local or network storage, Backing up to Acronis Cloud.
- To recover specific files and folders after they have been accidentally deleted or corrupted.

Recovery methods:

- **Full recovery** can be performed to the original location or to a new one.
  When the original location is selected, the data in the location is completely overwritten with the data from the backup. In case of a new location, the data is just copied to the new location from the backup.
- **Incremental recovery** is performed only to the original location and only from a cloud backup. Before the recovery starts, the files in the original location are compared with the files in the backup by file attributes, such as file size and date of last modification. Those files that do not match are marked for recovery, the remaining files will be skipped during recovery. In that way, as opposed to the full recovery, Acronis Cyber Protect Home Office recovers only changed files. This method significantly reduces the recovery time and saves Internet traffic while recovering from Acronis Cloud.

Backup versions

A backup version is created during a backup operation. Each version represents a point in time to which the system or data can be restored. The first backup version contains all the data selected for backup. The second and subsequent versions contain only data changes that occurred since the previous backup version. All the backup versions are stored in a single backup file.

Backup file format

When you back up your Mac to a local storage or a network place, Acronis Cyber Protect Home Office saves backup data in the proprietary .tib or .tibx format, by using compression. The data from .tib or .tibx file backups can be recovered only through Acronis Cyber Protect Home Office.

When you back up your Mac to Acronis Cloud, Acronis Cyber Protect Home Office saves your data "as is". You can recover the data in the product or via the Acronis Cloud web application on any Mac computer that has an Internet connection.

Schedule

For your backups to be really helpful, they must be as up-to-date as possible. Schedule your backups to run on a regular basis.

Backup retention rules

Every time you run a backup operation, manually or on a schedule, Acronis Cyber Protect Home Office creates a new backup version in the backup location. To delete obsolete backup versions automatically, you can set the backup retention rules. Refer to Cleaning up backups, backup versions, and replicas for details.

2.2 What you can and cannot back up

The table below shows what and where you can back up.

	Backup destinations							
	Internal drives (HDD, SSD, RAID)	Acronis Cloud	USB drives	Thunderbolt	AirPort Time Capsule	Network share, NAS	CD, DVD	FTP server
Internal drives (HDD, SSD)	+	+	+	+	+	+	-	-
USB drives	+	+	+	+	+	+	-	-
FireWire drives	+	+	+	+	+	+	-	-
Thunderbolt	+	+	+	+	+	+	-	-
Fusion Drive	+	+	+	+	+	+	-	-
Hard drives protected with FileVault 2	+	+	+	+	+	+	-	-
Hard drives with Boot Camp installed	+	+	+	+	+	+	-	-
Specific files	+	+	+	+	+	+	-	-
Separate partitions	-	-	-	-	-	-	-	-
RAID, Apple	-	-	-	-	-	-	-	-

RAID								
CD, DVD	-	-	-	-	-	-	-	-
APM disks	-	-	-	-	-	-	-	-

2.3 Backing up to local or network storage

1. Open Acronis Cyber Protect Home Office.
2. Perform one of the following:
   - If this is your first backup, skip this step.
   - If you already have a backup and you want to create a new one, click **Add Backup** at the bottom of the backup list.

     Note
     To delete a backup, right-click it, and then click **Delete**. The backup will be removed from the list and the backup files and the files of the backup replica will be permanently deleted from the backup storage. These files cannot be ever recovered.

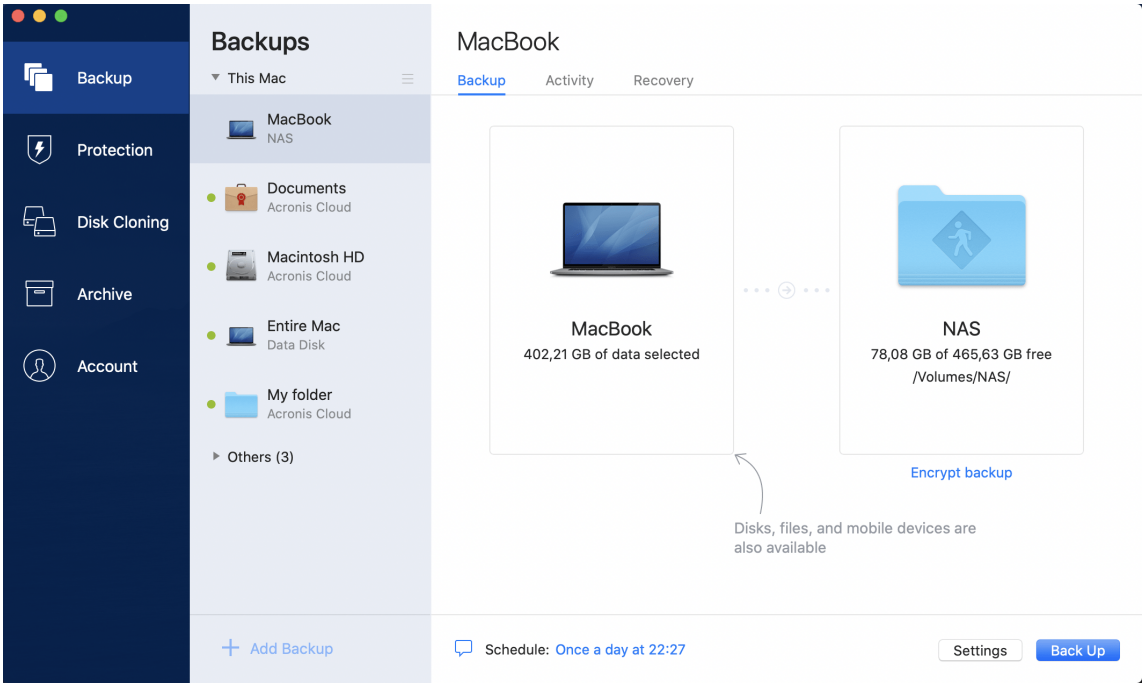
3. Click the backup source icon, and then select what you want to back up:
   - **Entire Mac**

     When you select this option, Acronis Cyber Protect Home Office backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents.
   - **Disks**
   - **Files and folders**
   - **Mobile device**

     Refer to Backing up mobile devices for details.
   - **Files to notarize**

     Refer to Notarized backup for details.

- **NAS** (if any connected)



4. Click the backup destination icon, select where you want to save the backup file to, and then click **OK**. If the location is not listed, click **Browse**, and then select a location.

   If you have an NAS device, it will be automatically detected and listed along with other locations.
5. [Optional step] Configure additional settings. You can:
   - Exclude files and folders manually at **Settings** —> **Exclusions**. Refer to Excluding items from backups for details.
   - Configure the backup schedule at **Settings** —> **Schedule**. Refer to Scheduling for details.
   - Set the backup retention rules at **Settings** —> **Cleanup**. Refer to Cleaning up backups, backup versions, and replicas for details.
   - Protect your backup with a password and encryption at **Settings** —> **Encryption**. Refer to Backup encryption for details.
6. After you have configured all settings and you are ready to start a backup, click **Back Up**.

To recover your Mac from a Acronis Cyber Protect Home Office backup, you must have an Acronis bootable media. If you do not have one, please create it. Refer to Creating Acronis bootable media for details.

2.4 What is Acronis Cloud?

Acronis Cloud is a secure remote storage which you can use to store your backups and archives. Because files are stored in a remote storage, you can recover the entire contents of your Mac if a disaster or data corruption event occurs.

If you use Acronis Cyber Protect Home Office for Windows, you can also store file backups, disk images, and versions of your synchronized files in Acronis Cloud.

To start using Acronis Cloud

1. Open Acronis Cyber Protect Home Office.
2. Create Acronis account, if you do not have one.
3. [optional] If Acronis Cloud doesn't not make part of your subscription, activate it as follows: on the left sidebar, click **Account**. Then, click **Activate Acronis Cloud**. In **Acronis Cloud Storage**, click **Try now** or **Buy**.

The Acronis Cloud website allows you to recover and manage the data that you store on Acronis Cloud. To access the website, go to https://www.acronis.com/my/online-backup/webrestore/, and log in to your account. .

2.4.1 Creating an Acronis account

To use the Acronis Cloud service, you need an Acronis account.

To create an Acronis account

1. Open Acronis Cyber Protect Home Office.
2. Select Acronis Cloud as a destination for your backup. The login window will open.
3. Click **Create Account**.
4. Fill in the registration form. Provide the required data, accept the Terms of Use, and, optionally, subscribe to receive news and promotional offers occasionally.

   Note
   To keep your personal data secure, choose a strong password for your account, guard it from falling into the wrong hands, and change it from time to time.

5. Click **Create Account**.
6. A message will be sent to the email address that you specified. Open this message and confirm that you wish to create an account.

2.4.2 Subscription to Acronis Cloud

The Acronis Cyber Protect Home Office features that use Acronis Cloud (such as online backup, cloud archiving, and data synchronization) require a subscription to Acronis Cloud Storage. To subscribe, open Acronis Cyber Protect Home Office, click **Account** on the left sidebar, and then choose the required subscription.

Note
Please note that Acronis Cloud is subject to our Fair Usage Policy. See more details at https://kb.acronis.com/ati/fairusage.

Trial version

When you activate the trial version of the product, a 1000 GB storage and free subscription to Acronis Cloud for the Acronis Cyber Protect Home Office trial period is assigned to your account automatically. After the trial subscription expires, Acronis Cloud works in recovery-only mode for 30

days. After this period, you won't be able to use the Acronis Cloud service and all your data on the Cloud will be deleted.

To purchase the full Acronis Cloud Storage subscription

1. Open Acronis Cyber Protect Home Office.
2. On the left sidebar, click **Account**. Then, click **Buy Now**.
3. Select the required subscription, and click **Buy Now**.
4. Follow the on-screen instructions to proceed with the purchase.

You can also buy the full subscription at the Acronis website.

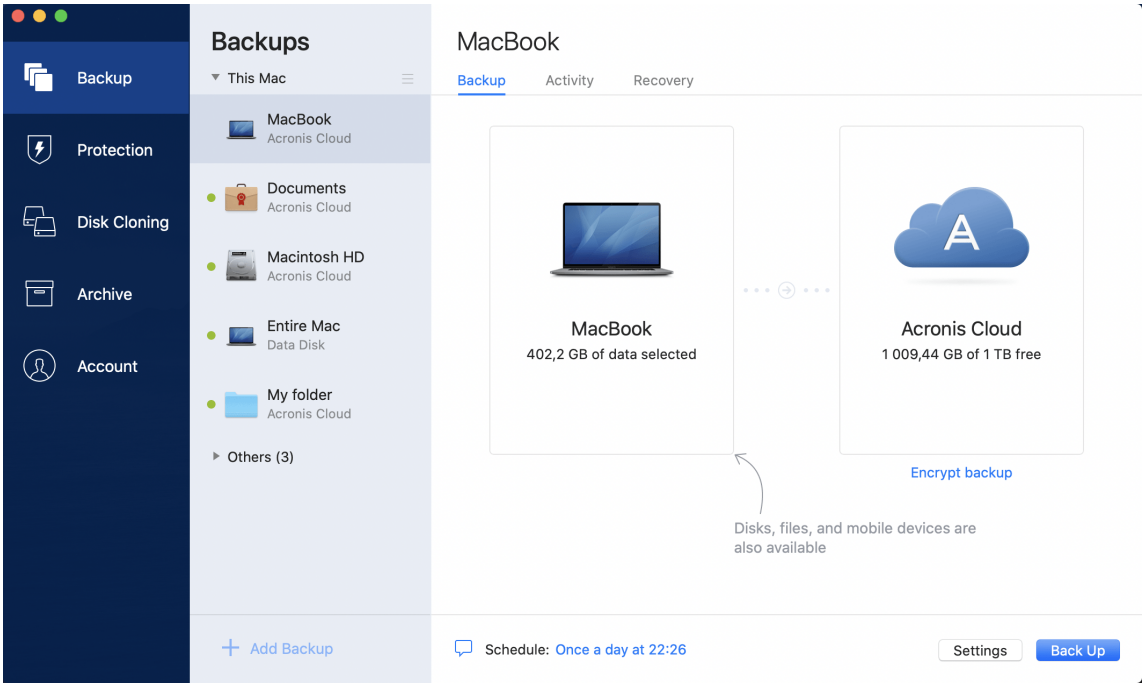
2.5 Backing up to Acronis Cloud

1. Open Acronis Cyber Protect Home Office.
2. Perform one of the following:
   - If this is your first backup, skip this step.
   - If you already have a backup and you want to create a new one, click the plus sign at the bottom of the backup list.

     Note
     To delete a backup, right-click it, and then click **Delete**. The backup will be removed from the list and the backup files will be permanently deleted from the backup storage. These files cannot be ever recovered.

3. Click the backup source icon, and then select what you want to back up:
   - **Entire Mac**
     When you select this option, Acronis Cyber Protect Home Office backs up all your internal hard drives in disk mode. The backup contains the operating system, installed programs, system settings, and all your personal data including your photos, music, and documents.
   - **Disks**
   - **Files and folders**
   - **Mobile device**
     Refer to Backing up mobile devices for details.
   - **Cloud service**
     Used to back up Office 365 data.
   - **Files to notarize**
     Refer to Notarized backup for details.

- NAS device (if any connected)



4. Click the backup destination icon, select Acronis Cloud, and then click **OK**.

   If you are not signed in yet, enter the email address and password of your Acronis account, and then click **Sign In**.

   If you do not have an Acronis account, click **Create Account**, type your email address, password, and then click the **Create Account** button. Refer to Creating an Acronis account for details.
5. [Optional step] Configure additional settings. You can:
   - Exclude data protected with third-party services, if you use any. Click **Optimize backup** and specify the data to exclude. Refer to Excluding items from backups for details.
   - Exclude files and folders manually at **Settings** —> **Exclusions**. Refer to Excluding items from backups for details.
   - Configure the backup schedule at **Settings** —> **Schedule**. Refer to Scheduling for details.
   - Set the backup retention rules at **Settings** —> **Cleanup**. Refer to Cleaning up backups, backup versions, and replicas for details.
   - Protect your backup with a password and encryption at **Settings** —> **Encryption**. Refer to Backup encryption for details.
   - Select a preferred data center and configure the upload speed at **Settings** —> **Network**. Refer to Network settings for backup for details.
   - Configure the backups attempts at **Settings** —> **Error Handling**.
6. After you have configured all settings and you are ready to start a backup, click **Back Up**.

Note
The first online backup may take a considerable amount of time to complete. Future backup processes will likely be much faster, because only changes to files will be transferred.

To recover your Mac from a Acronis Cyber Protect Home Office backup, you must have an Acronis bootable media. If you do not have one, please create it. Refer to Creating Acronis bootable media for details.

2.6 Replicating local backups to Acronis Cloud

2.6.1 Why replicate?

Even though backing up your data provides protection, we recommend that you also replicate all local backups to Acronis Cloud, to protect from incidental corruption of your computer. Of course, you can create two backup plans, one to backup to your local computer and another one to Acronis Cloud. But automatic replication saves time when setting up the backup plans and creating a replica is faster than creating another backup. A replica is a copy of your backup and it can be used as a safeguard and accessed from anywhere.

2.6.2 Replication activation

Replication is not activated by default. You can activate it for any backup of a disk, partition or entire computer that uses the local destination (to an external or internal disk) that you configured in Acronis True Image 2020 or higher. You can activate the replication in a special tab of a backup plan.

To activate the replication of a backup to Acronis Cloud

1. From the backup list, select the backup that you want to replicate, and then open the **Replica** tab.
2. Click **Replicate**. Now, replication is activated and will start once the normal backup is created. You are free to close Acronis Cyber Protect Home Office. Both the backup and replication processes will continue in background mode.
3. [optional step] Open the **Backup** tab, click **Settings**, and then click **Replication** to configure the cleanup settings for Acronis Cloud to optimize usage of its space.

2.7 Notarized backup

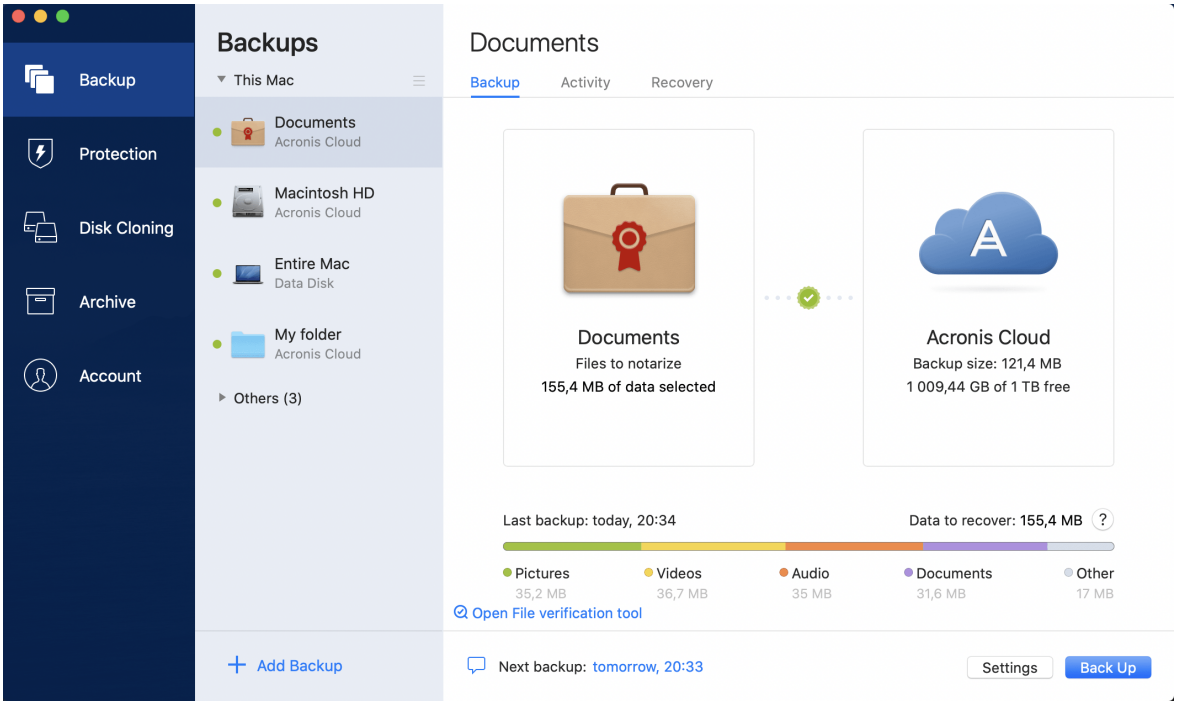
By using Blockchain technology, Acronis Cyber Protect Home Office can protect your files from unauthorized modification. This gives you a guarantee that you can recover your data from the same file that was backed up. We recommend that you use this type of backup to protect your legal document files or any other files that require proved authenticity. Refer to Using Blockchain technology for details.

To create a notarized backup of your files and folders

1. Open Acronis Cyber Protect Home Office.
2. Perform one of the following:
   - If this is your first backup, skip this step.
   - If you already have a backup and you want to create a new one, click **Add Backup** at the bottom of the backup list.

Note
To delete a backup, right-click it, and then click **Delete**. The backup will be removed from the list, and the backup files will be deleted from the backup storage.

3. Click the backup source icon, click **Files to notarize**, and then select the files and folders that you want to back up.



4. Click the backup destination icon, select where you want to save the backup file to, and then click **OK**. If the location is not listed, click **Browse**, and then select a location.

   If you have an NAS device, it will be automatically detected and listed along with other locations.
5. [Optional step] Configure additional settings. You can:
   - Exclude files and folders manually at **Settings** —> **Exclusions**. Refer to Excluding items from backups for details.

     To exclude files with a digital signature from the backup, select the **Do not notarize digitally signed files** check box. Refer to Excluding items from backups for details.
   - Configure the backup schedule at **Settings** —> **Schedule**. Refer to Scheduling for details.
   - Protect your backup with a password and encryption at **Settings** —> **Encryption**. Refer to Backup encryption for details.
   - Select a preferred data center and configure the upload speed at **Settings** —> **Network**. Refer to Network settings for backup for details.
6. After you have configured all settings and you are ready to start a backup, click **Back Up**.

2.7.1 Using Blockchain technology

Acronis Cyber Protect Home Office uses the Blockchain technology to provide top-level security for your backed-up files. This technology gives you the guarantee that your files have not been modified

by fraudulent software, and when it is time to recover, you recover data from exactly the same file that was backed up.

What is Blockchain?

Blockchain is a database that contains information about transactions and their sequence. In general, a transaction represents an event, such as a financial operation or an operation with different kinds of assets. The transactions are united in blocks, which are written to the database one by one and form a block chain. Every transaction and every block has its own unique identification number. What is very important is that every block stores information about all previous blocks of the chain. Once written to the database, the information about a transaction cannot be changed in any way or by anyone, and the transaction sequence cannot be modified either. Any attempt to change any piece of information in the database can be easily identified by any user of the database, because there would be no information about the false transaction or false block in all subsequent blocks. This technology guarantees that data stored in the database is valid, belongs to a specific person, and has not been modified by anyone. See more information about Blockchain at https://en.wikipedia.org/wiki/Blockchain_(database).

How Acronis Cyber Protect Home Office uses the Blockchain technology

To protect your files from unauthorized modification, Acronis Cyber Protect Home Office uses the Acronis Notary technology. This is a universal solution for timestamping and fingerprinting any data objects and streams. Since it is impractical to store large amount of data in a Blockchain database, Acronis Cyber Protect Home Office sends only file hash codes to the Acronis Notary service.

A hash code is a unique number of fixed size that is produced by a hash function. The code mathematically defines an arbitrary set of data, for example, a backup file. Any change of the backup file leads to a change of its hash code. Therefore, to check if the file was changed, you only need to compare the hash codes generated in the initial and current states of the file. If the codes match, this is a guarantee that the file has not been modified by anyone.

When Acronis Notary receives hash codes of your files, it calculates a new single hash code and sends it to the Ethereum Blockchain-based database. See more information about Ethereum at https://www.ethereum.org/.

Once the hash code is in the database, the files that were used to calculate this hash code are notarized by Acronis Notary. You can easily verify the file authenticity at any time by using the procedure described in Verifying file authenticity. Every notarized file has a notarization certificate, which is documentary proof that the file is protected with the Blockchain technology. A certificate contains general information about the file and technical details that allow you to manually verify the file authenticity. Refer to Manual verification of a file's authenticity for details.

2.7.2 Verifying file authenticity

By using Blockchain technology, Acronis Cyber Protect Home Office can protect your backed-up files from unauthorized modification. This gives you a guarantee that you can recover data from exactly

the same file that was backed up.

To verify a file's authenticity in Acronis Cyber Protect Home Office

1. Open Acronis Cyber Protect Home Office.
2. On the sidebar, click **Backup**.
3. From the backup list, select the notarized backup which contains the file that you want to verify.
4. On the right panel, open the **Recovery** tab.
5. Browse to the required file, click the arrow icon, and then click one of the following:
   - **View certificate**—The certificate containing the detailed information about the file security will be opened in the web browser.
   - **Verify**—Acronis Cyber Protect Home Office will check the file authenticity.

To verify a file's authenticity in File verification tool

1. Open the File verification tool with one of the following methods:
   - In a web browser, open https://notary.acronis.com/verify.
   - On the sidebar of Acronis Cyber Protect Home Office, click **Backup**, select a notarized backup, and then click **Open File verification tool** on the right panel.
2. In Finder, browse to the file that you want to verify, and then drag it to the web browser window.

To verify a file's authenticity in Acronis Cloud

1. Go to https://www.acronis.com/my/online-backup/webrestore/, and then log in to your Acronis account.
2. On the sidebar, click **Backups**.
3. From the backup list, select the notarized backup which contains the file that you want to verify.
4. Browse to the required file and select it with a check mark. Then, click **Verify** on the right sidebar.

2.7.3 Manual verification of a file's authenticity

The easiest way to verify a file's authenticity is to use the **Verify** command in Acronis Cyber Protect Home Office or in the Acronis Cloud web application. Refer to Verifying file authenticity for details. In addition to this easy method, you can perform the verification procedure yourself, step by step.

To verify a file's authenticity manually

Step 1. Calculate MD5 hash of the file

1. Open Terminal.
2. For example, to calculate the md5 hash for the picture.png file, type:

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

   Example of an md5 hash: eea16ade1edf2750a46bb6bffb2e45a2
3. Check that the calculated md5 hash is equal to an eTag in the DATA field in your notarization certificate. Refer to Verifying file authenticity for details about obtaining a file certificate.

Step 2. Check that a ROOT is stored in the blockchain

1. Open a blockchain explorer, for example https://etherscan.io/.
2. Enter the TRANSACTION ID from the certificate into the search field.
3. Check that the Data field in the Event Logs tab is equal to the ROOT value in your certificate.

Step 3. Check that the hash is included in the tree

1. Download the command line utility from the GitHub repository: https://github.com/acronis/notary-verifyhash/releases.
2. Follow the instructions at: https://github.com/acronis/notary-verifyhash.

2.8 Backing up mobile devices

If you have an iOS or Android smartphone, you can use Acronis Cyber Protect Home Office to protect your mobile data such as photos, video files, contacts, and calendars. Refer to Acronis Mobile documentation for details.

To back up mobile data to local storage on your computer

1. Make sure that:
   - Acronis True Image 2017 or a later version, or Acronis Cyber Protect Home Office, is installed on your computer.
   - The Acronis Mobile app is installed on your mobile device.
   - Your mobile device and your computer are connected to the same Wi-Fi network.
2. On your computer:
   a. Start Acronis True Image 2017 or a later version, or Acronis Cyber Protect Home Office.
   b. On the sidebar, click **Backup**, and then click **Add Backup**.
   c. Click the **Backup source** area, and then select **Mobile device**.
   A QR code will be displayed. Please do not close this window.
3. On your mobile device:
   a. Start Acronis Mobile.
   b. Tap a plus icon to create a backup. Note that this step does not occur the first time you back up your mobile device.
   c. Select computer as a backup destination.
   d. Tap **Scan QR code**, point your camera at the QR code on the computer screen, and then wait until the mobile device is connected to the computer.
   e. Select the data categories that you want to back up, or tap **Confirm** if you want to back up all of them.
   f. Allow Acronis Mobile to access to your personal data.
   g. [optional step] Enter a password to encrypt the backup and protect it. Otherwise, tap **Skip Encryption**.
   h. Tap **Start Backup**.

When the backup is started, you can track the progress in any application - on the computer or mobile device, but the errors and warning messages are displayed in the mobile app only.

You can close Acronis True Image or Acronis Cyber Protect Home Office on your computer and the Acronis Mobile app. The backup will continue in the background mode.

When the backup is complete, your data is uploaded to your computer. If you want data changes (for example, new photographs) to be backed up automatically, make sure the **Continuous backup** setting is turned on. If this setting is turned off, the new data is backed up only when you tap **Back up**.

The connection between your computer and mobile device may be lost because of an error. To restore it, select the mobile backup in the backup list of Acronis Cyber Protect Home Office, click **Reconnect**, and then scan the QR code with your mobile device. After that, the backup will continue normally with the same settings.

2.8.1 Acronis Mobile

Note
Acronis Cloud might be unavailable in your region. For more information, click here: https://kb.acronis.com/content/4541

Acronis Mobile allows you to back up your data to Acronis Cloud, to local storage on your computer, and then recover it in case of loss or corruption. Note that backup to the cloud storage requires an Acronis Cloud subscription.

Which devices does the mobile app support?

You can install Acronis Mobile on any mobile devices that runs one of the following operating systems:

- iOS 11 and later (iPhone, iPad, iPod)
- Android 6.0 and later (mobile phones only)

Key features

Acronis Mobile allows you to:

- Back up your personal data, including:
  - Photos
  - Videos
  - Contacts
  - Calendars
  - Messages (Android only)
  - Reminders (iOS only)
- Choose the following locations as a backup destination:
  - Acronis Cloud
  - Local storage on your PC or Mac
- Encrypt backups with the AES-256 cryptographic algorithm

- Automatically back up new and changed data
- Access cloud backups from all your mobile devices and recover data from these backups

Where can I find these apps?

You can view additional information and download Acronis Mobile from the Apple App Store or Google Play:

- Acronis Mobile for iOS devices: https://go.acronis.com/atimobile/download/iOS
- Acronis Mobile for Android devices: https://go.acronis.com/atimobile/download/Android

2.8.2 Local destination of mobile backups

When you back up your mobile data to a computer, Acronis Cyber Protect Home Office stores the backups in the default folder */Library/Application Support/Acronis Mobile Backup Data/acronis-local-data/*. When you change the default folder, the *acronis-local-data* folder is moved to the location that you selected. All new mobile data will be backed up to the new location.

Note
All mobile backups are always stored in the same folder and cannot be separated.

To change the local destination for mobile backups

1. In the **Backup** section, right-click a mobile backup, and then click **Move**.
2. Click **Select location**, and then select a new location for the backups. Note, you can select a location only on your internal hard drives.

To change the new location to the initial one, click **Reset to default**.

2.9 Backing up Office 365 data

2.9.1 Why back up Office 365 data?

Even though Microsoft Office 365 for Home is a set of cloud services, regular backups provide an additional layer of protection from user errors and intentional malicious actions. With Acronis Cyber Protect Home Office, you can protect your Microsoft Outlook mailboxes and Microsoft OneDrive data by backing up them to secure Acronis Cloud. After uploading to Acronis Cloud, all of the content is available from any device, any time. You can recover deleted items from a backup even after the Office 365 retention period has expired.

2.9.2 Backing up Office 365 data

Data that you can back up in your Outlook mailbox:

- All folders
- E-mail messages
- Attachments

Note
You cannot back up shared or group mailboxes.

Data that you can back up in your OneDrive:

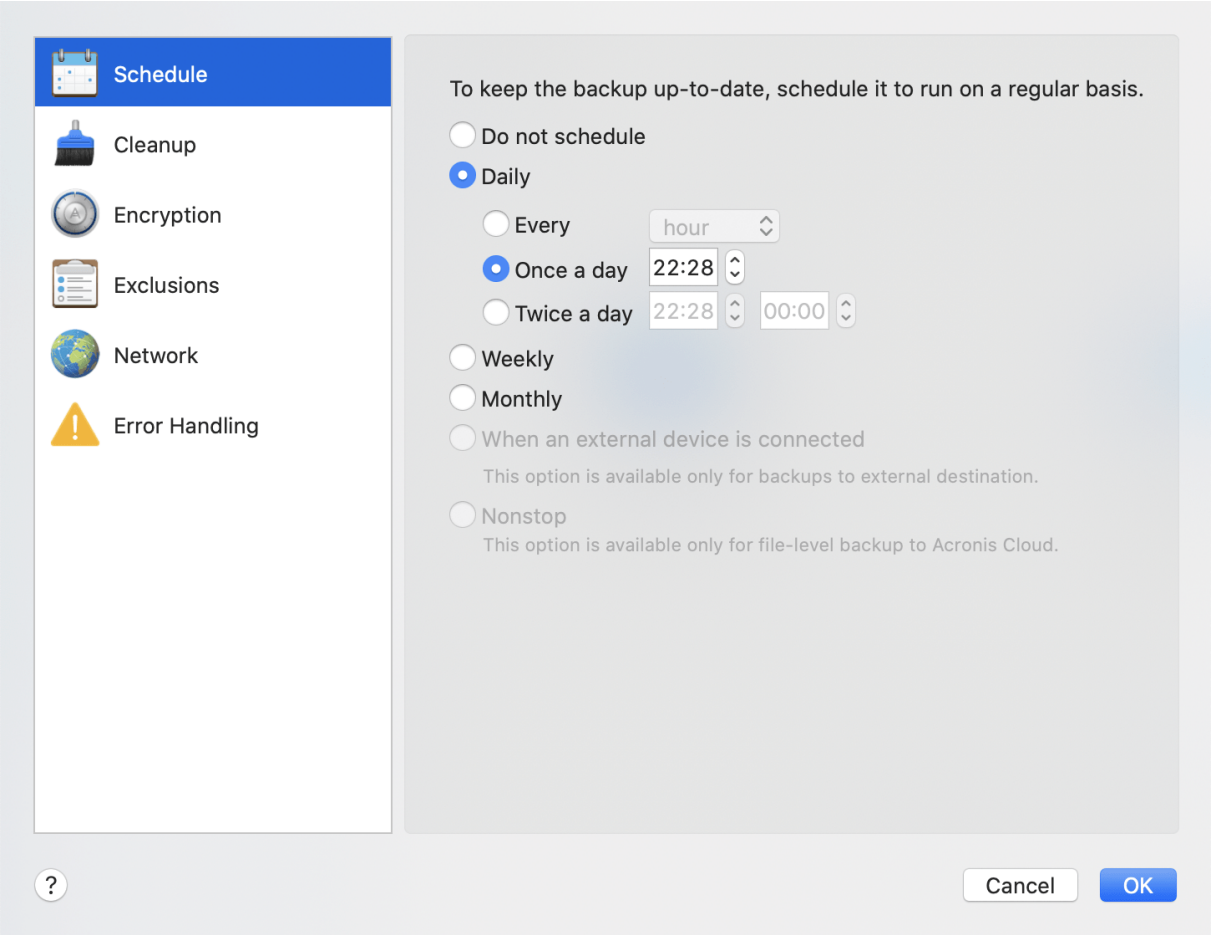
- All files and folders

To back up Office 365 data:

1. Open Online Dashboard by doing one of the following:
   - Follow the link: https://cloud.acronis.com.
   - On the sidebar of Acronis Cyber Protect Home Office, click **Backup**, click **Add backup**, click the **Backup source** area, and then select **Cloud service**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, click **Add**, and then choose **Microsoft Office 365 for Home**.
4. Log in to your Microsoft account, if prompted.
5. At the **Backup source** area, select items to backup:
   - Entire account
   - Outlook
   - OneDrive
6. Click **Done.**
7. You can configure cleanup rules for the backup via the **Cleanup** pane. You can also encrypt the backup and protect it with a password. When done, click **Apply**.
8. To start the backup, click **Run now**.

2.10 Scheduling

For your backups to be really helpful, they should be as up to date as possible. Schedule your backups to run on a regular basis. By default, your Mac is backed up daily.



To schedule the backup

1. Click **Settings**, choose backup frequency, and then specify the start time.
   - **Do not schedule**

     This option turns scheduling off.
   - **Daily**

     The backup starts once or twice a day at the specified time or with a time interval that you select.
   - **Weekly**

     The backup starts every week on the selected days and at the specified time.
   - **Monthly**

     The backup starts every month on the selected dates and at the specified time.
   - **When an external device is connected** (available for backups to external destination only)

     If you schedule a task for performing backup to a USB flash drive or external HDD, the backup starts every time the same external device is attached. Select the **Once a day** check box if you want the backup to be performed only once a day for the device.
   - **Nonstop** (available for file-level cloud backup only)

     The initial full backup contains all of the data selected for protection. Acronis Cyber Protect Home Office then continually monitors the protected files (including open ones). Once a

modification is detected, the changed data is backed up. The shortest interval between the incremental backup operations is five minutes. This allows you to recover your data to an exact point in time.

2. After you have configured all settings, click **OK**.

If your Mac is switched off or it is in the sleep mode when the scheduled time comes, the backup will run the next time the Mac starts or when it wakes up. You can use Mac Power Nap to avoid gaps in backing up your data.

2.10.1 To use Mac Power Nap

- Turn on the Power Nap in your mac **Energy Saver** > **Power Adapter** parameters.
- In the Acronis Cyber Protect Home Office menu, click **Preferences**, click **General**, and then select the **Back up when your Mac is in Power Nap** check box. Click **OK**.

When this setting in turned on, and your Mac is in the sleep mode when the scheduled time comes, the backup will run in the next Power Nap. Please be aware that backing up during Power Nap works only if your computer is connected to the power supply.

2.11 Backup encryption

To protect the backed up data from unauthorized access, you can encrypt the backup with industry-standard AES (Advanced Encryption Standard) cryptographic algorithm with a 256-bit long key.

Note
You cannot change the backup encryption option for a pre-existing backup.

To encrypt a backup

1. When configuring the first backup process, click the **Settings** icon, and then click **Encryption**.
2. Enter the password for the backup into the corresponding field, and then click **OK**.
   We recommend that you use a password longer than seven symbols and containing both letters (in upper and lower cases preferably) and numbers to make it more difficult to guess.
   A password cannot be retrieved. Please memorize the password that you specify for a backup protection.

2.12 Cleaning up backups, backup versions, and replicas

Every time you run a backup operation, manually or on a schedule, Acronis Cyber Protect Home Office creates a new backup version in the backup location.

When you want to delete backup versions that you no longer need, use the tools provided in the application. If you delete backup version files outside Acronis Cyber Protect Home Office, for example in File Explorer, this will result in errors during operations with the backups.

Versions of the following backups cannot be deleted manually:

- Backups stored on CD, DVD, BD, or Acronis Secure Zone
- Nonstop backups
- Notarized backups

Nonstop backup retention rules

When you back up files and folders to Acronis Cloud, you can select the nonstop scheduling setting. Refer to Scheduling for details.

Because Acronis Cyber Protect Home Office permanently monitors the backed-up data and uploads the changes to Acronis Cloud, the backup could consume storage space quite fast. To reduce the number of backup versions and optimize the cloud space consumption, Acronis Cyber Protect Home Office keeps only the following backup versions:

- All versions for the last hour
- The first versions of every hour for the last 24 hours
- The first version of every day for the last week
- The first version of every week for the last month
- The first version of every month

All other versions are automatically deleted. The retention rules are pre-set and cannot be changed.

Replica retention rules

Every time you run a backup operation that has replication turned on, Acronis Cyber Protect Home Office creates a new backup version locally and a new replica version in the cloud. Sometimes the number of replica versions is slightly less that the number of the backup versions; that is done to optimize your Internet usage. Nevertheless, the replicas may take quite a lot of space. To save space, use the replica retention rules:

1. In the **Backup** section, click the required backup, and then click **Settings** in the lower-right corner.
2. Click **Settings**, choose **Replication**.

You can set a limit on the number of replica versions. In addition to the number of replicas, you can limit their age. Select the **Delete versions older than** check box, and then specify how long to store a version. All versions that are older than the specified period will be automatically deleted.

To delete an entire backup and its replica

In the **Backup** section, right-click the backup with the replica to delete, and then click **Delete backup and replica**.

Depending on the backup type, this command completely deletes the backup from its location, or allows you to choose whether you want to delete the backup completely or delete the backup box only. When you delete a backup box only, the backup files remain in the location and you will be able to add the backup to the list later. Note that if you delete a backup completely, the deletion cannot be undone.

When you delete a backup, its replica is deleted automatically. You cannot delete a local backup and still save its replica. However, you can delete a replica alone and keep the corresponding local backup.

To delete a replica without deleting the backup, in the **Backup** section, right-click the backup with the replica to delete, and then click **Delete replica only**.

To configure cleanup settings

1. In the **Backup** section, click the required backup, and then click **Settings** in the lower-right corner.
2. Select the **Cleanup** tab and configure the cleanup settings.

By default, Acronis Cyber Protect Home Office stores 20 recent versions. When you create the twenty-first version, Acronis Cyber Protect Home Office automatically deletes the oldest version of the backup. You can set a different limit on the number of backup versions.

2.13 Cleaning up space on Acronis Cloud

1. On the sidebar, click **Account**, and then click **Browse my data**. The Acronis Cloud web application opens.
2. On the left sidebar of the web application, click **Account**.
3. On the Acronis Cloud line, click **Clean up**.
4. Choose which versions you want to delete:
   - Versions older than some period.
   - All old versions except for several recent ones.

Warning!
Be careful! Deleted versions cannot be restored.

One more way to clean up is to delete a cloud backup that you no longer need. In this case, all version history for the backup is deleted from Acronis Cloud.

2.14 Adding an existing backup to the list

You may have Acronis Cyber Protect Home Office backups created by a previous product version or copied from another computer. Every time you start Acronis Cyber Protect Home Office, it scans your computer for such backups and adds them to the backup list automatically.

If you have backups that are not shown in the list, you can add them manually.

To add backups manually

1. In the **File** menu, point to **Add Existing backup**. The program opens a window where you can browse for backups on your computer.
   Also, you can use Spotlight to search by .tib or .tibx files.
2. Select a backup version (a .tib or .tibx file). The entire backup will be added to the list.

You can restore data from all backups in the list. You can also reconfigure backups created on the same Mac.

To reconfigure a backup

1. Click the backup source icon, and then select what you want to back up.
2. [Optional step] Schedule your backup to run on a regular basis.
3. To start the backup, click **Back Up**.

Note
If you want to hide some local backup from the list, right-click it, and then click **Hide from the list**. You will not be able to do any operations with this backup until you add it again manually.

2.15 Excluding items from backups

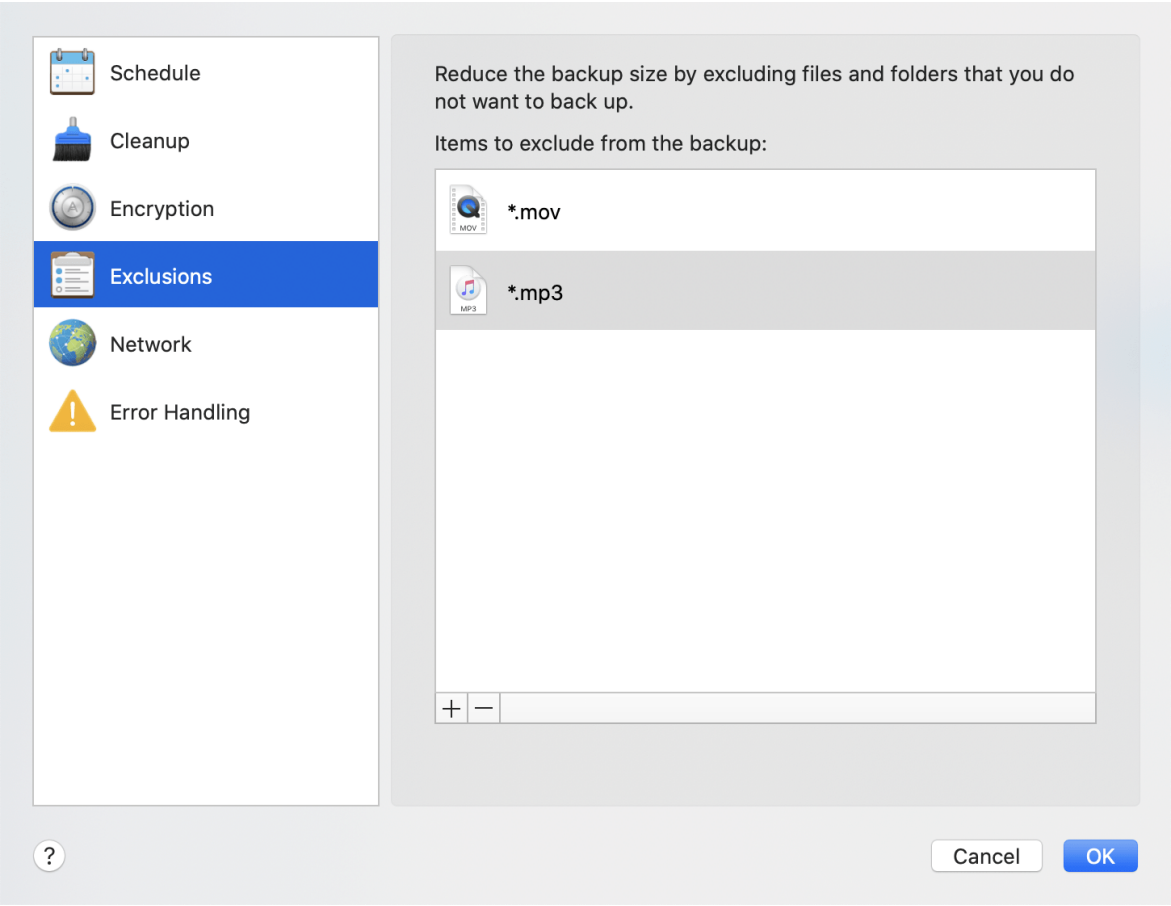
Before you start a backup, you can reduce the backup size by excluding data that does not need to be backed up.

You can exclude files and folders the following ways:

- **Manually, from any backup**
  To exclude an item, specify it explicitly or use a mask.
- **Automatically, from a backup to Acronis Cloud**
  Acronis Cyber Protect Home Office analyzes the backup source and suggests that you exclude your local data that can be downloaded from third-party Cloud storage.

2.15.1 Excluding items manually

1. When configuring a backup, click **Settings**, and then click **Exclusions**.



2. Click the Plus sign, and then click one of the following:
   - **Exclude specific file or folder**

     Browse to the item that you want to exclude, select it, and then click **Exclude**.
   - **Exclude by mask**

     Enter an exclusion mask by using wildcard characters (* and ?), and then click **Exclude**.

     Examples of exclusion masks:
     - **.ext* - all files with an .ext extension will be excluded.
     - *??name.ext* - all files with an .ext extension, having six letters in their names starting with any two symbols (??) and ending with *name*, will be excluded.
3. Select or clear the **Do not notarize digitally signed files** check box (available for notarized backups only).

   The main purpose of a notarized backup is protection of your personal files. Therefore, there is no need to back up system files, application files, and other files that have a digital signature. To exclude these files, select the corresponding check box.
4. Click **OK**.

2.15.2 Excluding recoverable data from online backups

Acronis Cyber Protect Home Office allows you to exclude your local data that is uploaded or synchronized with third-party Cloud services, such as Google Drive or Dropbox. This data is already reliably protected and can be easily downloaded to your computer. Therefore there is no need to upload it to Acronis Cloud. You can exclude it to reduce the backup size and to speed up the backup process.

You can exclude data protected with the following services:

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

Acronis Cyber Protect Home Office suggests that you exclude data only when the following conditions are met:

- The third-party service is currently enabled.
- There is more than 250 MB of data stored in the corresponding folder.

To exclude items from an online backup

1. Before you start the backup process, click **Optimize backup** below the backup source icon.
2. Select the check boxes next to the items that you want to exclude, and then click **Done**.

2.16 Connection settings

If you are connecting to a networked computer or an NAS device, in most cases you will need to provide the necessary credentials for accessing the network location. For example, this is possible when you select a backup destination. Then, if the credentials to the location are modified, you need to correct them manually in the backup settings. Otherwise, all further backup operations will fail.

To change credentials to a network location

1. Open Acronis Cyber Protect Home Office.
2. In the **Backup** section, select the backup that has a network location as a source or destination.
3. Click the gear icon to open the backup settings.
4. In the **Connection** section, specify the user name and password to access the network location.
5. [Optional step] Click **Test connection**.
   If the connection has been established, the credentials are correct.
6. Click **OK** to apply the changes.

2.17 Network settings for backup

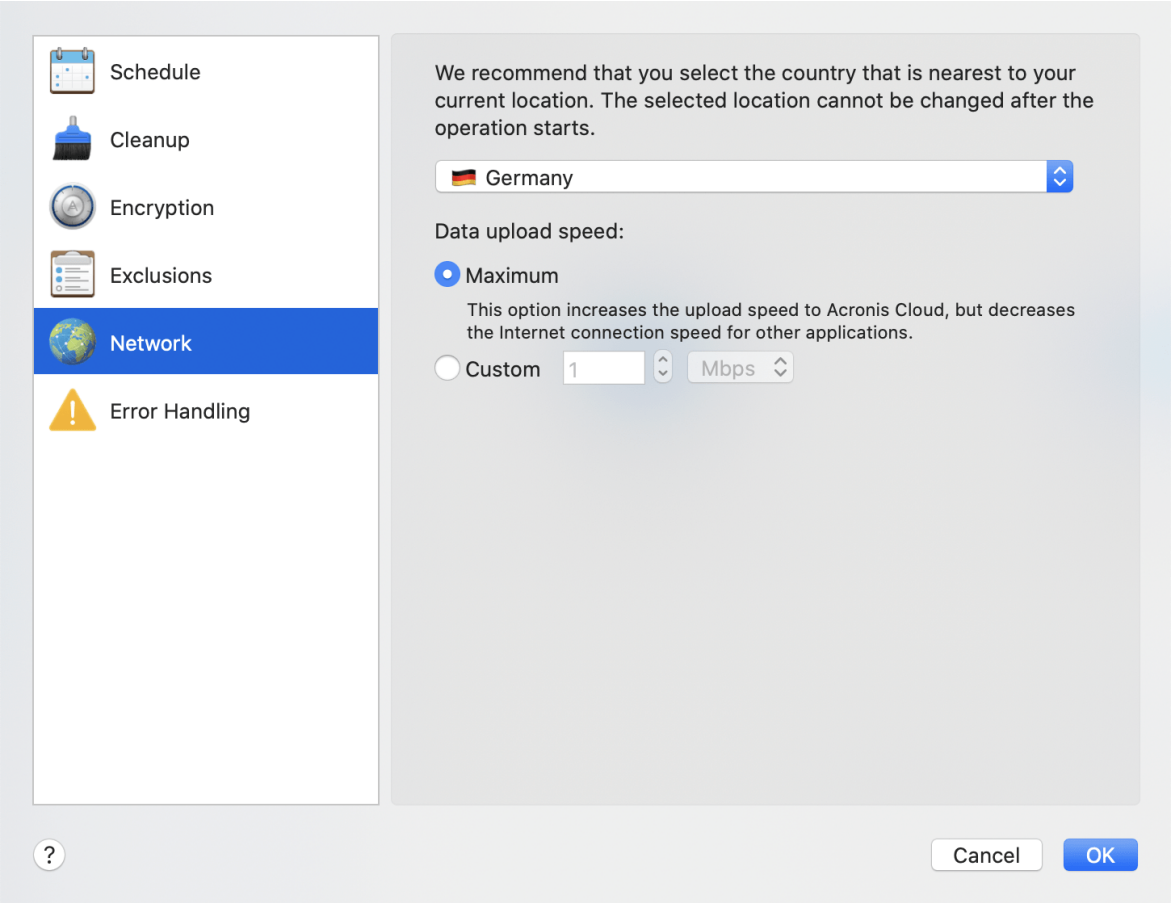
When you create a backup to Acronis Cloud, your data is uploaded to one of the Acronis data centers located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your online backups and synced files are stored in the same data center, by default.

We recommend that you set the data center for a backup manually, when you are in a different country and your default data center is not the closest to your current location. This will significantly increase the data upload rate.

Note
You cannot change the data center for an already existing backup.

To select a data center

1. When configuring an online backup, click **Settings**, and then click **Network**.



2. Select the country that is closest to your current location, and then click **OK**.

2.17.1 Data upload speed

When you back up data to Acronis Cloud, you can change the connection speed used by Acronis Cyber Protect Home Office. Set the connection speed that will allow you to use Internet and network resources without annoying slowdowns.

1. In the backup settings, go to the **Network** section.
2. To set up the connection speed, select one of the following options:
   - **Maximum**—The data transfer rate is maximum within a system configuration.
   - **Custom**—You can specify a maximum value for data upload speed.

2.18 Backup activity and statistics

On the **Activity** tab and the **Backup** tab, you can view additional information on a backup, such as backup history and file types the backup contains. The **Activity** tab contains a list of operations performed on the selected backup starting from its creation, the operation statuses, and statistics. This comes in handy when you need to find out what was happening to the backup in background mode, for example the number and statuses of scheduled backup operations, size of backed-up data, etc.

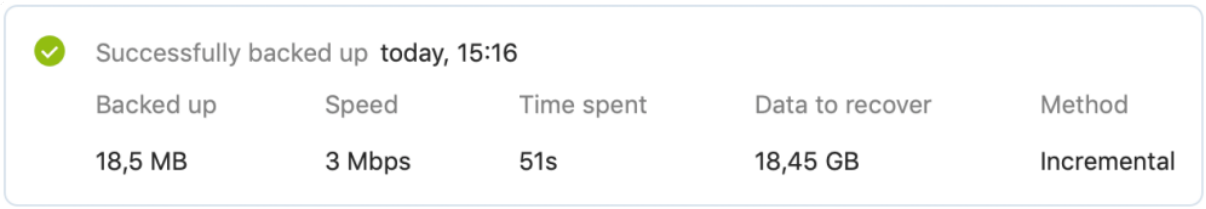
When you create the first version of a backup, the **Backup** tab displays a graphical representation of the backup content by file types.

2.18.1 The Activity tab

Note
Nonstop backup and mobile backups do not have an activity feed.

To view a backup activity

1. On the sidebar, click **Backup**.
2. In the backup list, select the backup, the history of which you want to view.
3. On the right pane, click **Activity**.



What you can view and analyze:

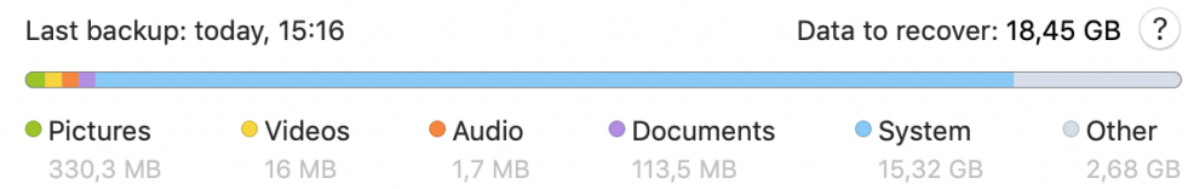
- Backup operations and their statuses (successful, failed, canceled, interrupted, and so on)
- Operations performed on the backup, and their statuses
- Error messages

- Backup comments
- Backup operation details, including:
  - **Backed up**—Size of backed-up data, with compression.
  - **Speed**—Backup operation speed.
  - **Time spent**—Time spent for the backup operation.
  - **Data to recover**—Initial size of data, without compression.
  - **Method**—Backup operation method (full, incremental).

For more information, refer to the Knowledge Base article: https://kb.acronis.com/content/60104.

2.18.2 The Backup tab

When a backup is created, you can view statistics on types of the backed-up files:



Point to a color segment to see the number of files and the total size for each data category:

- Pictures
- Video files
- Audio files
- Documents
- System files
- Other file types, including hidden system files

Data to recover shows the size of the original data that you selected to back up.

2.19 Laptop power settings

Note
This setting is only available on computers with batteries (laptops, computers with UPS).

When you work on your laptop and there is no power supply around you or when your computer has switched to UPS after a blackout, it's reasonable to save the battery charge. Sometimes long-term backups may consume the battery power quite fast.

To save the battery charge

- In the Acronis Cyber Protect Home Office menu, click **Preferences**, then click **Battery Saver**, and then select the **Do not back up when battery power is less than** check box. Then click **OK**.

When this setting is turned on, if you unplug your laptop power adapter or use a UPS for your computer after a blackout, and the remaining battery charge is equal or below the level in the slider,

all current backups are paused and scheduled backups will not start. Once you plug the power adapter back in or the power supply is restored, the paused backups will be resumed. The scheduled backups that have been missed because of this setting will be started as well.

This setting does not block backup functionality completely. You can always start a backup manually.

Local mobile backups do not depend on this setting. Your mobile data is backed up to local storage on your computer as usual.

2.20 Wi-Fi networks for backup to Acronis Cloud

When you back up your data to Acronis Cloud, you can be concerned about the security of your personal data when it is transferred by unprotected Wi-Fi networks. To avoid the risk of theft of your personal data, we strongly recommend that you only use protected Wi-Fi networks.

To protect your data

- In the Acronis Cyber Protect Home Office menu, click **Preferences**, click **Wi-Fi networks**, and then select **Back up using only selected Wi-Fi networks**. In the **Remembered networks** box which contains all remembered Wi-Fi networks, select the check boxes next to the networks that you want to use to back up your data.

When the networks are selected and your computer loses a connection to any of them, all current backups are paused and scheduled backups will not start. Once the computer connects to any of these networks, the suspended backups will be resumed. The scheduled backups that have been missed because of this setting will be started as well.

To back up your data by using a new Wi-Fi network, simply save this network on your computer and then select it in the **Remembered networks** box. This can be done whenever you need to use new network.

Local mobile backups do not depend on this setting. Your mobile data is backed up to local storage on your computer, as usual.

2.21 Notifications

2.21.1 Notifications in macOS Notification Center

You can duplicate Acronis Cyber Protect Home Office notifications in macOS Notification Center to view them in their usual place and without opening the Acronis Cyber Protect Home Office console. The notifications in macOS Notification Center will display automatically.

To duplicate in-product notifications in Notification Center, in the Acronis Cyber Protect Home Office menu, click **Preferences**, and then select the **Show notifications in Notification Center** check box.

2.21.2 Notifications in Acronis Tray Notification Center

When Acronis Cyber Protect Home Office is open, you can see the status of any operation in it. However, since some operations can take quite a while, such as a backup, there is no need to keep Acronis Cyber Protect Home Office to learn its result. The notifications in macOS Notification Center stay open until you close them, but you cannot open a notification that has been closed. To view the information, you need to open Acronis Cyber Protect Home Office.

The Tray Notification Center contains latest notifications in one place, lets you see important operation statuses without opening Acronis Cyber Protect Home Office at the moment when you need them. The following notifications are shown in Acronis Tray Notification Center: personal offers, information on the results of backup operations, and other important notifications from Acronis Cyber Protect Home Office. The Tray Notification Center is minimized and hidden under Acronis Cyber Protect Home Office in the Mac tray.

2.21.3 Email notifications about backup status

When you cannot wait a backup completion or when you want to track your scheduled backups, it is convenient to receive the backup status reports on your email address. This allows you to be immediately informed if anything goes wrong with your backups even when you are not near your computer.

To configure email notifications

1. In the Acronis Cyber Protect Home Office menu, click **Email Notification Settings**.
   The **Email notifications** page of the Online Dashboard opens in your web browser.
2. Select message types that you want to receive.
3. Type email address to send the notifications to.
4. Type a message subject template by using the following variables:
   - [computer_name]
   - [operation status]
   - [backup_name]

   For example, you can type: *Backup report: [backup_name] - [operation status] on [computer_name]*
5. Click **Save**.

2.22 Parallels Desktop support

2.22.1 What is Parallels Desktop?

Parallels Desktop is an application that allows you to run different operating systems on your Mac, by using a special virtual environment. It is usually used to run Windows, but you can also run macOS, Linux, Google Chrome OS, and other operating systems. For more details, please visit the Parallels website: https://www.parallels.com/products/desktop/.

2.22.2 How does Acronis Cyber Protect Home Office handle Parallels Desktop virtual machines?

Acronis Cyber Protect Home Office provides complete support of your virtual machines created with Parallels Desktop 16 or higher. When you back up your Mac, the virtual machines are backed up as well. When you recover your Mac, the virtual machines revert to the state they were in when the backup started. After recovery, all your virtual machines remain consistent and bootable.

2.22.3 How does it work?

Every time you run a backup, Acronis Cyber Protect Home Office creates snapshots of all Parallels Desktop virtual machines stored on the disks or in the folders selected to back up. These snapshots are used as time points to revert to when you recover your Mac. After the created snapshots are stored in the backup, they are automatically deleted from your Mac.

2.22.4 Which virtual machines are backed up?

Acronis Cyber Protect Home Office backs up all virtual machines that are:

- Stored on the disks being backed up
- Added to the Parallels Desktop application
- Currently running, stopped, and suspended

2.22.5 How do I recover virtual machines?

If your virtual machines were created with Parallels Desktop 16 or higher, all restored virtual machines will boot after recovery. If you used an earlier version of Parallel Desktop, you should run the recreate_pd_hdd.sh script to restore the bootability of your recovered machines.

Since Acronis True Image 2017, this script is shipped with the product and is located in /Applications/Acronis Cyber Protect Home Office.app/Contents/MacOS/recreate_pd_hdd.sh.If you use an earlier version, download the script file from: https://kb.acronis.com/system/files/content/2016/08/49198/recreate_pd_hdd.zip.

To run the script

1. Unpack the .zip file of the script.
2. Open Terminal.
3. Type *bash "[script_path]" "[vm_path]"*, where
   - [script_path] is a path to the script file.
   - [vm_path] is a path to the folder, where the recovered virtual machine files are located.

   For example:

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

Note
We recommend recovering the PD machines as new virtual machines and rather than overwriting the previous ones.

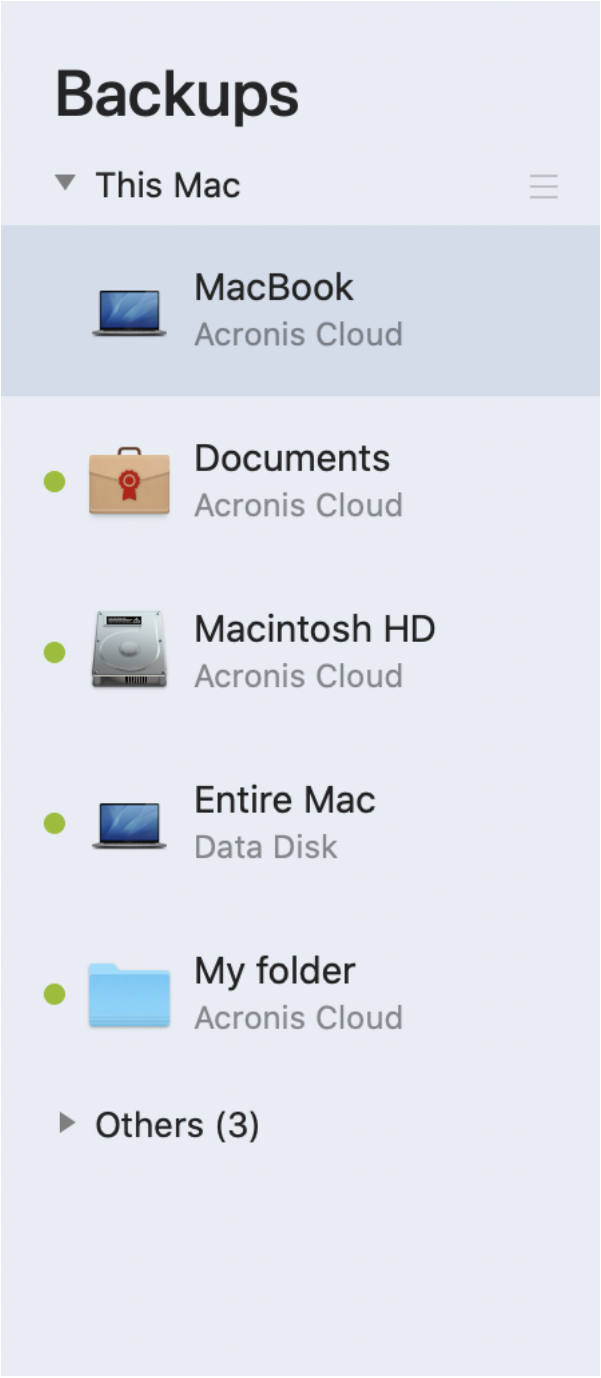
2.22.6 Limitations

If you have Parallels Desktop virtual machines configured to use the Boot Camp partition, pay attention to the following limitations:

- If the virtual machine is running, backup of the Boot Camp partition will fail in most cases.
- If the virtual machine is suspended, backup of the Boot Camp partition will succeed, but recovery from the backup will fail in most cases.
- If the virtual machine is suspended, recovery to the Boot Camp partition will fail. Instead, remove the Boot Camp partition, and then recover it from the backup to the unallocated space.

2.23 Backup list

While working with the backup list, you will see special icons. The icons give you a backup type and backup current state.



2.23.1 Backup states

Icon	Description
●	The backup successfully completed.
●	The backup is queued.
●	The backup is in progress.

Icon	Description
(blinking)	
○	The backup was paused by user.
●	The last backup failed.
●	The backup completed with warnings.

2.23.2 Sorting backups in the list

By default, the backups are sorted by the date they were created, starting from the newest to oldest. To change the order, select the appropriate sorting type in the upper part of the backup list. You have the following options:

Command		Description
Sort by	**Name**	This command sorts all backups in alphabetical order. To reverse the order, select **Z —> A**.
	Date created	This command sorts all backups starting from newest to oldest. To reverse the order, select **Oldest on top**.
	Date updated	This command sorts all backups by date of the last version. The newer the last backup version, the higher the backup will be placed in the list. To reverse the order, select **Least recent on top**.
	Size	This command sorts all backups by size, from biggest to smallest. To reverse the order, select **Smallest on top**.
	Source type	This command sorts all backups by the source type.
	Destination type	This command sorts all backups by the destination type.

3 Creating bootable media

3.1 Creating Acronis bootable media

Acronis bootable media is a removable drive containing boot files. When your Mac does not start, you use the drive to boot the Acronis recovery environment and recover your Mac from a previously created backup.

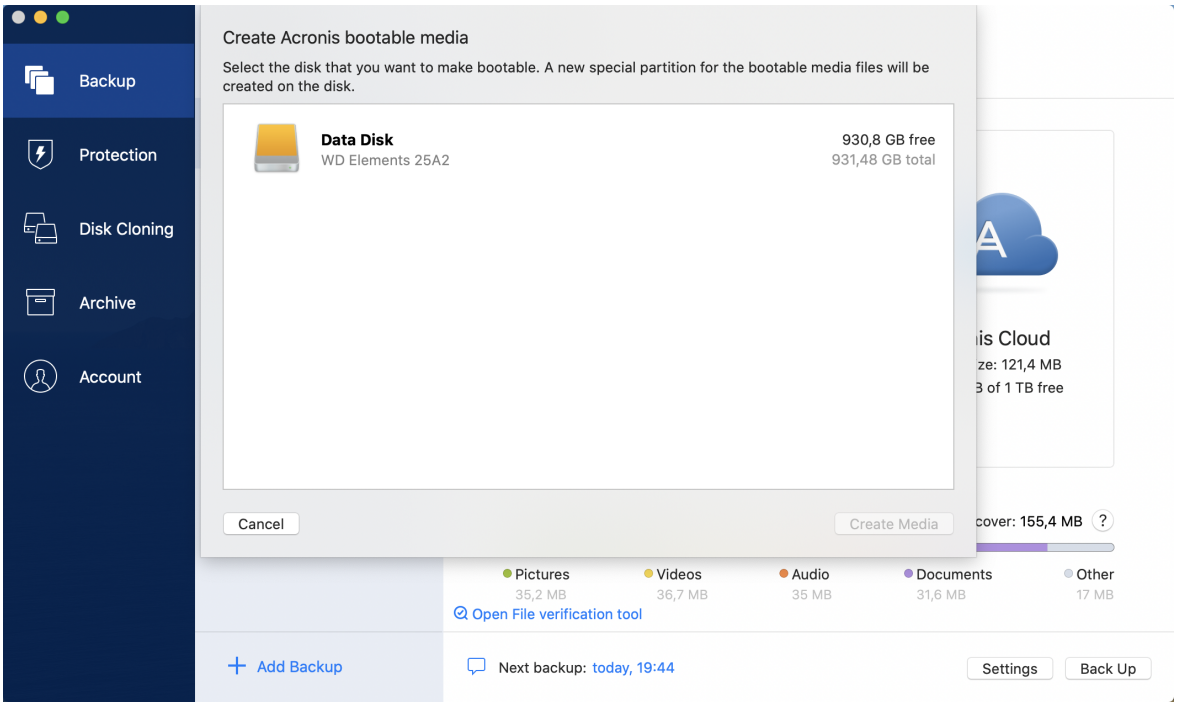
Note
Fusion Drive is not supported as target for Acronis bootable media and Acronis Survival Kits.

If you do not have a backup yet, please create it. Refer to Backing up to local or network storage, Backing up to Acronis Cloud. .

Warning!
Using Acronis bootable media is the only way to recover your Mac from an Acronis Cyber Protect Home Office backup.

To create Acronis bootable media

1. Connect a removable drive to your Mac.
   The drive must have at least 4 GB of free space. For example, you can use an external hard drive or a USB flash drive. The drive will be formatted with the Mac OS Extended file system. Note that CD and DVD media are not supported.
2. Open Acronis Cyber Protect Home Office.
3. In the **File** menu, click **Create Acronis Bootable Media**. In the opened window, click **Create Media**.
4. The Acronis Media Builder window opens.



5. Select the drive that you want to make bootable.
6. Click **Create Media**.

   Acronis Cyber Protect Home Office creates a small partition on the selected drive and writes the boot files there. To create it, one of the existing volumes will be resized. If the disk is not a GPT one and it has a file system different from Mac OS Extended or APFS, Acronis Cyber Protect Home Office suggests formatting the disk. Pay attention, as disk formatting deletes all the data stored on the disk.
7. When the process is completed, disconnect the media and keep it in a safe place. You can store your own data on the media, but make sure that you do not delete or modify the Acronis boot files.

Note
We recommend that you create a new bootable media every time you upgrade your macOS to a newer version. Otherwise, your bootable media may not work properly.

3.2 Creating an Acronis Survival Kit

3.2.1 What is an Acronis Survival Kit?

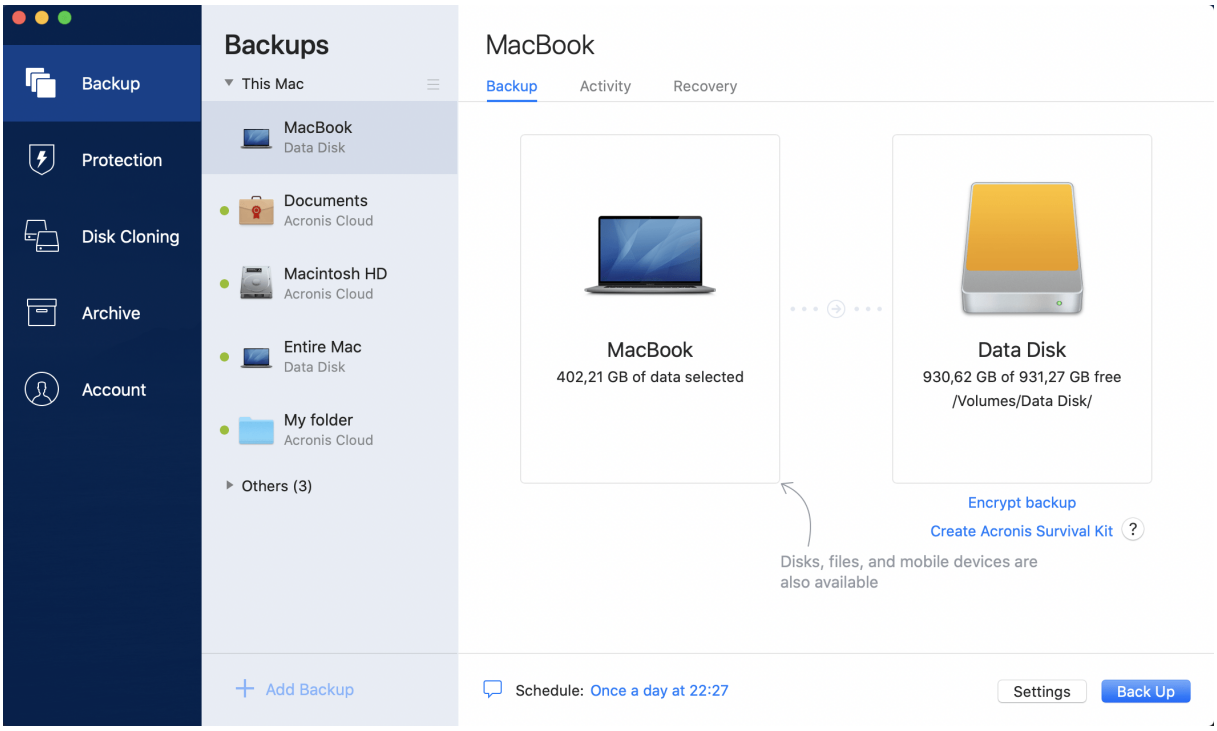
To recover your Mac in case of a failure, you need to have two crucial components—a backup of your system disk and a bootable media. Most often these components are separated, for example, the system backup is stored on an external drive or Acronis Cloud and the bootable media is a small USB flash drive. Acronis Survival Kit combines both components so that you could have a single device that has everything that you need to recover your computer in case of a failure. It is an external hard drive that contains both the Acronis bootable media files and a backup of your system partition or entire computer.

As a device for an Acronis Survival Kit you can use an external hard drive that is larger than 32 GB and has Mac OS Extended or APFS file system. If the drive has another file system, Acronis Cyber Protect Home Office suggests formatting the drive.

Note
Fusion Drive is not supported as target for Acronis bootable media and Acronis Survival Kit.

3.2.2 How do I create an Acronis Survival Kit?

When you configure a local backup of your system or entire Mac and select an external drive as a destination, Acronis Cyber Protect Home Office will suggest making this drive bootable.



To create an Acronis Survival Kit

1. Click **Back Up** or **Create Acronis Survival Kit**.
2. In the opened window, click **Create**.
   Acronis Cyber Protect Home Office creates a small partition on the selected drive and writes the boot files there. To create it, one of the existing volumes will be resized. If the disk is not a GPT one and has a file system different from Mac OS Extended or APFS, Acronis Cyber Protect Home Office suggests formatting the disk. Pay attention, that disk formatting deletes all the data stored on the disk.
3. When the boot files are successfully written to the drive, it becomes a bootable media that you can use to recover your Mac. To complete creating an Acronis Survival Kit, you need to save a backup of your system to the drive. To do this, click **Back Up**. If you skip this step, do not forget to create a system backup on this drive later. Refer to Backing up to local or network storage for details.

When your Acronis Survival Kit is ready, you can use it to recover your Mac. Refer to Recovering your Mac for details.

4 Recovery

4.1 When do I recover my Mac?

When your computer does not start up or you notice that your macOS or some applications do not work properly, in most cases that means that it's time to recover your operating system from the disk image. First though, we recommend that you determine the source of the problem.

System errors can be due to two basic factors:

- **Hardware failure**
  In this scenario, it is better to let your service center handle the repairs.
- **Corruption of an operating system, applications or data**
  When the failure cause is a virus, malware or corruption of system files, recover the system from the backup. Refer to Recovering your Mac for details.

To determine source of the problem

1. Check the cables, connectors, power of external devices, etc.
2. Restart your Mac. Press and hold the **Option** key while the Mac is starting. The recovery menu will be displayed.
3. Choose **Disk Utility** from the list, and then click **Continue**.
4. Select the disk that you want to check, and then click **First Aid**.
   If the Disk Utility informs you that the disk is going to fail, the cause is due to the physical condition of the disk. For example, it may contain bad sectors. We recommend that you back up the disk as soon as possible, and then replace it.
5. Click **Verify Disk**.
   - If there is an error, click **Repair Disk**. If the Disk Utility reports that the disk is OK or it has been repaired, restart your Mac and continue using it as usual. If the errors persist, recover your Mac from a Acronis Cyber Protect Home Office backup. Refer to Recovering your Mac for details.
   - If the Disk Utility does not detect any errors, recover your Mac from a Acronis Cyber Protect Home Office backup. Refer to Recovering your Mac for details.

4.2 Recovering your Mac

Follow the instructions below to recover your Mac when it cannot start or when it is working incorrectly.

1. Make sure that you have:
   - A previously created Acronis Cyber Protect Home Office backup. Without the backup recovery is impossible. Refer to Backing up to local or network storage and Backing up to Acronis Cloud for details.

- Acronis bootable media. If you do not have one and you can start Acronis Cyber Protect Home Office on your Mac, please create the media as soon as possible. Refer to Creating Acronis bootable media for details.

2. Plug in the bootable media to your Mac.
3. To display the boot menu:
   - [On an Intel-based Mac] Start or restart your Mac. Press and hold the Option key while the Mac is starting.
   - [On a Mac with Apple silicon] Shut down your Mac. Press and hold the power button.
4. Choose Acronis Bootable Media as a device to boot from. The utilities are displayed.
   - [On an Intel-based Mac] Select **Recover from Acronis Cyber Protect Home Office Backup**, and then click **Continue**.
   - [On a Mac with Apple silicon] Select **Acronis Bootable Media**, and then click **Restore**.
5. In the window that opens, choose the location of your backup:
   - **Acronis Survival Kit**
   - **Local Storage**
   - **Acronis Cloud**—sign in to your account.
   - **Network**

   Select your backup, and then click **Open**.
6. From the list, select the backup version from which you want to recover your Mac, and then click **Next**. The contents of the version are displayed.
7. Select the check boxes next to the partitions that you want to recover. Select a destination for each partition.

Note
If Acronis Cyber Protect Home Office automatically determines a destination for each partition in the backup, the simplified view appears. You cannot make changes in this mode. If you need to select partitions manually, click the **Advanced View** button.

8. To start recovery, click **Recover**, and then confirm that you want to erase all data on the destination partitions.
9. [For Big Sur] When prompted, click **Restore Data** if you only need to restore data on an unbootable data volume. Click **Restore with Reboot** if you need a bootable volume with macOS

installed. Note that it requires internet connection.

10. [Except Big Sur] When recovery is complete, restart your Mac.

4.2.1 FAQ about Boot Camp partition

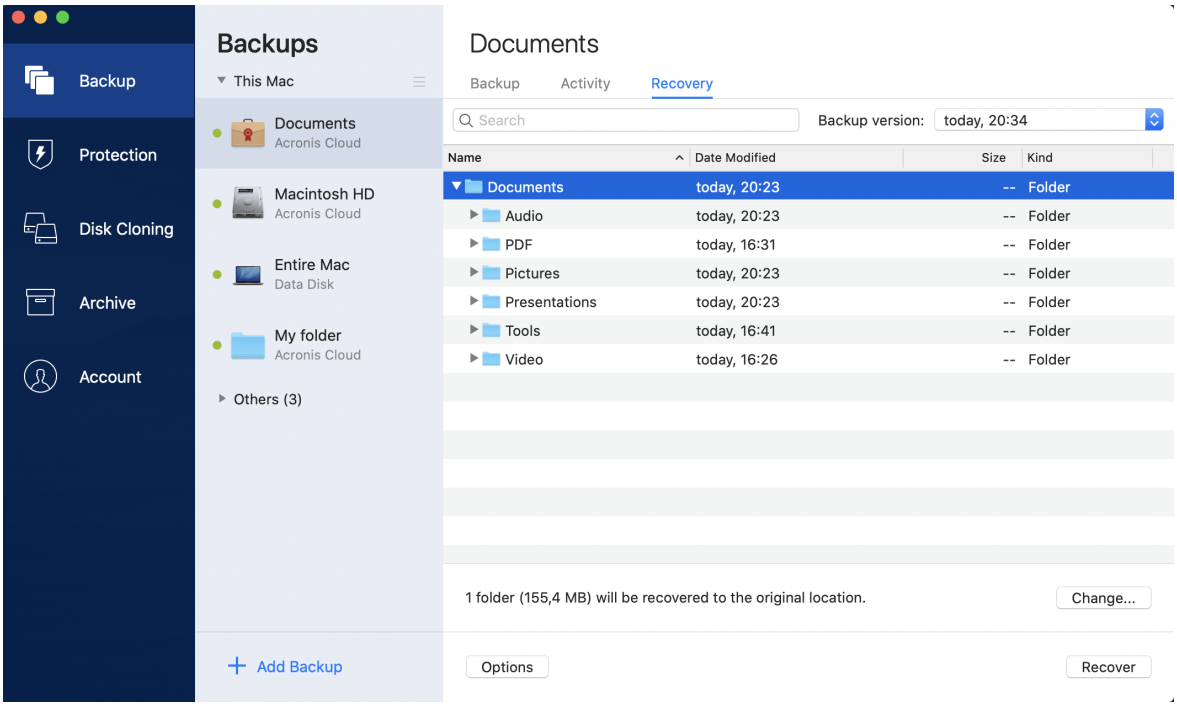
- **How do I back up my Boot Camp partition?**
  Back up the hard drive where Boot Camp is installed. The backup will contain all the data stored on the drive, including the Boot Camp partition.
- **Can I back up my Boot Camp partition separately?**
  No, you can't. Acronis Cyber Protect Home Office allows you to create disk-level backups only. Back up the hard drive that contains the Boot Camp partition, instead.
- **How do I recover my Boot Camp partition?**
  You can do this in the bootable media environment. At the recovery source and destination selection step, select all the listed partitions. This will recover the entire hard drive. To recover the Boot Camp partition only, select the check box next to this partition, and then clear all other check boxes.
- **Can I resize my Boot Camp partition before recovery?**
  No, you can't. The Boot Camp partition remains the same size as it is in the backup.
- **What recovery destinations can I select for a Boot Camp partition?**
  We strongly recommend that you recover your Boot Camp partition to itself, though you can select any recovery destination.
- **Can I recover specific files from the backed up Boot Camp partition?**
  Yes, you can recover them without limitations, the same way that you would recover any other files.
- **I want to replace my hard drive with a new one. Can I clone macOS, the Boot Camp partition, and all of my data to the new hard drive?**
  Yes, you can. Do the following:
  1. Back up your hard drive to an external storage media, for example, a USB drive or a network share.
  2. Turn off your Mac, and then replace your old hard drive with a new one.
  3. Boot your Mac by using Acronis bootable media.
  4. Recover your Mac from the backup to the new hard drive.

4.3 Recovering your files and folders

Follow the instructions below when you need to recover specific files and folders from a backup.

To recover data in Acronis Cyber Protect Home Office:

1. On the left pane, select the backup that contains the files and folders to recover, and then open the **Recovery** tab.
   The window with the backup contents opens.



2. In the **Backup version** list, select the backup version by its backup date. When you complete the procedure, the files and folders will be recovered to the state they were in on that date.
3. Select the files or folders that you want to recover.
4. [Optional step] By default, the selected files or folders will be recovered to the original location. To recover to a custom location, click **Change** and browse to the location that you want to use for the recovery.
5. [Optional step, available for cloud backups only] Click **Options**, and then configure file recovery options. Refer to File recovery options for details.
6. Click **Recover**. When the progress is complete, your data is recovered to the selected date and time and stored in the original or custom location.

   In case of notarized backup, Acronis Cyber Protect Home Office will additionally verify the authenticity of the recovered files.

To recover data in Acronis Cloud

You can recover specific files and folders from an online backup stored on Acronis Cloud. To perform this operation, you first need to open the Acronis Cloud web site.

To open the Acronis Cloud website

– On your Mac with Acronis Cyber Protect Home Office installed

1. Open Acronis Cyber Protect Home Office.
2. On the left pane, select **Account**.
3. In the Acronis Cyber Protect Home Office section, **Browse my data**.

– On a computer or mobile device with an Internet connection:

1. In your web browser, go to https://www.acronis.com/my/online-backup/webrestore/.
2. Log in to your Acronis account.

The web application opens in your web browser.

To recover files and folders

1. On the **Backups** tab of the Acronis Cloud web application, click the required backup name. Then, browse to the file or folder that you want to recover. You can also use the **Search** field. Select the required file or folder with a check mark.
2. [Optional] To recover a specific version of a file (not a folder), click **Versions** on the right sidebar. Then, select the required date and time of the backup, and click the download icon on this line.
3. To start recovery, click **Download**.

The selected data will be downloaded to the default downloads folder.

4.4 Recovering Office 365 data

Acronis Cyber Protect Home Office allows you to protect your personal Office 365 account from losing your e-mail messages, files and folders, profile information, and other data. When you have a cloud backup of your account data, you can browse it and recover specific items.

4.4.1 What items can be recovered?

The following items can be recovered from a mailbox backup:

- Entire mailbox
- E-mail messages
- Attachments

The following items can be recovered from a OneDrive backup:

- Entire OneDrive
- Any files and folders that were backed up

4.4.2 Recovering Office 365 data

To browse and recover your data

1. Open Online Dashboard by doing one of the following:
   - Follow the link: https://cloud.acronis.com.
   - On the sidebar of Acronis Cyber Protect Home Office, click **Account**, and then click **Open Online Dashboard**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, find the Office 365 backup box, and then click **Recover**.
4. Browse a list of your backups. If needed, use the filter to find a backup by content.
5. After selecting a backup, click **Recover...**, and choose the data that you want to restore:

- Entire OneDrive or specific files and folders.
- Entire mailbox or specific messages.

When you choose to recover specific items, the Online Dashboard opens the list of the backed-up items. You can browse them, view their contents, and use search to find a specific item (not available for some data types).

After selecting items, you can choose an operation to perform (depending on data type, some operations may be unavailable):

- **Show content**—click to view the item details or open it in full size.
- **Send as email**—click to send the message to selected recipients.
- **Show versions**—click to view the versions of the item.
- **Recover**—click to specify a location for the items that you recover. You can also recover sharing permissions for some items.
- **Download**—click to download the selected file.

6. Click **Start recovery**.

4.5 Searching backup content

While recovering data from local backups, you can search for specific files and folders stored in the selected backup.

To search for files and folders

1. Start recovering data as described in Recovering files from local or network storage.
2. When selecting files and folders to recover, enter the file or folder name into the **Search** field. The program shows search results.

   You can also use the wildcard characters: * and ?. For example, to find all files with extension **.exe**, enter ***.exe**. To find all .exe files with names consisting of five symbols and starting with "my", enter **My???.exe**.
3. By default, Acronis Cyber Protect Home Office searches the folder selected on the previous step. To include the entire backup in the search, click **Entire Backup**.

   To return to the previous step, click the cross icon.
4. After the search is complete, select the files that you want to recover, and then click **Next**.

Note
Pay attention to the **Version** column. The files and folders that belong to different backup versions cannot be recovered at the same time.

4.6 File recovery options

You can select the following file recovery options for backups stored in Acronis Cloud:

- **Preserve file permissions** - selecting this option will preserve all the security properties (permissions assigned to groups or users) of the backup files. By default, files and folders are saved in the backup with their original security settings (i.e. permissions for read, write, execute

and so on for each user). If you recover a file/folder on a computer backed up under a different user account, you may not be able to read or modify this file.

If you clear this option and recover files to the current user home folder the recovered files/folders owner will be the current user.

- **Overwrite existing files** (available for file/folder level cloud backups only) - selecting this option will overwrite the files on the hard disk with the files from the backup if they are different. If your files or folders had recent changes that you want to keep when restoring, select the **Do not overwrite more recent files and folders** option.

5 Disk cloning

5.1 Clone disk utility

The usual copy operation does not make your new hard drive identical to the old one. For example, if you open Finder and copy all files and folders to the new hard drive, macOS will not start from the new hard drive. The Clone disk utility allows you to duplicate all your data and make macOS bootable on your new hard drive. As a result, your new disk becomes an exact clone of your old one.

When you need it:

- You have bought a new iMac or MacBook and you want to transfer all your data, including macOS, from your old Mac to the new one.
- You want to make an external drive a portable clone of your Mac's hard drive. You will be able to connect this external drive to any Mac and boot it to instantly make this Mac an exact copy of your own one.

What drives you can use:

- Internal system drive of your Mac (can be used as a source disk only)
- Internal non-system drive of your Mac
- Internal drive of another Mac
- External drive
- USB flash drive

If the destination drive is larger or smaller than the source one, the partitions of the source drive will be proportionally resized on the destination drive to fully occupy its space. The only exception is partitions smaller than 1 GB. Those partitions will not be resized.

It is not necessary that the destination disk is of the same size as the source one, it can be bigger or smaller, but its overall size must be larger than the used space of the source disk plus 10%. For example, you have a 1000 GB hard drive in your Mac, only 200 GB is used. If you want to clone it, the destination drive size must be 200+10%=220 GB, or larger. If your destination drive is too small, try deleting some unnecessary data from the source drive or moving the data to an external drive, USB flash drive. You can also move the data to cloud storage.

5.2 Cloning disks

The usual copy operation does not make your new hard drive identical to the old one. For example, if you open Finder and copy all files and folders to the new hard drive, macOS will not start from the new hard drive. The Clone disk utility allows you to duplicate all your data and make macOS bootable on your new hard drive. As a result, your new disk becomes an exact clone of your old one. Refer to Clone disk utility for details.

Important
To clone a Mac with Apple silicon, you must first clone the data to an external disk. Then, transfer the data from the external disk to the destination Mac.

To clone a disk

1. If you have Parallels Desktop virtual machines running on your Mac, make sure that they are turned off.
2. Make sure that the source and destination drives are connected to your Mac. If you need to connect another Mac, make sure that it is connected in target disk mode. Refer to Connecting two Macs for details.
3. Open Acronis Cyber Protect Home Office.
4. On the sidebar, click **Disk Cloning**, and then click **Continue**.
5. By default, your internal system drive is pre-selected as a cloning source. If you want to change it, click the cloning source icon, and then select the drive that you want to clone.
6. Connect the destination drive.

   Note
   Note that APM disks are not supported. If you have an APM disk, we suggest converting it to GPT or to MBR.

7. Click the cloning destination icon, and then select the destination drive for the cloned data.

   Warning!
   When you start the cloning operation, the destination drive will be formatted, and all of the data stored on it will be irreversibly erased. Make sure that the disk is empty or does not contain valuable data.

8. Click **Clone**.

Additional steps for a Mac with Apple silicon

1. Connect the clone disk to the destination Mac.
2. Shut down your destination Mac, then hold down the **Power** button until you see the startup options.
3. To configure macOS recovery, click **Options**.
4. Select **Disk Utility**. In the toolbar, click **Show All Devices**.
5. Select your Mac's internal disk and click **Erase** in the toolbar. Select the APFS format and confirm erasing. After that, your Mac will be restarted.
6. Activate your Mac. After that, exit to Recovery Utilities.
7. Select **Reinstall macOS Big Sur** and follow the steps to install macOS on the internal disk.
8. When macOS boots for the first time, configure the system settings.
9. In the **Migration Assistant** window, select to transfer data **From a Mac, Time Machine backup or Startup disk**.

10. In the **Transfer information to this Mac** window, select the cloned disk.
11. In the **Select the information to transfer** window, select all the information displayed, and create a password.
12. Install Acronis Cyber Protect Home Office on your Mac.

If the cloning operation is stopped for some reason, you will have to configure and start the procedure again. You will not lose your data, because Acronis Cyber Protect Home Office does not alter the original disk and data stored on it during cloning.

5.2.1 Cloning a Fusion Drive

A **Fusion Drive** is a hybrid drive that combines a relatively slow hard disk drive (HDD) with a fast solid-state drive (SSD). On your Mac you see the Fusion Drive as a single logical volume with the space of both drives combined.

Acronis Cyber Protect Home Office allows you to clone a Fusion Drive either to a Fusion Drive or to any other target drive.

To clone a Fusion Drive

1. If you have Parallels Desktop virtual machines running on your Mac, make sure that they are turned off.
2. Please ensure that the source and destination drives are connected to your Mac. Disconnect all unnecessary external devices.
3. Open Acronis Cyber Protect Home Office.
4. On the sidebar, click **Disk Cloning**, and then click **Continue**.
5. Select a Fusion Drive as a cloning source.
6. Connect the destination drive.
7. Click the cloning destination icon, and then select the destination drive for the cloned data.
   When you have more than one disk, the **Create a Fusion Drive** check box appears[1]. Select it, if you want to create a Fusion Drive, and then choose two disks. Confirm your choice.

   Warning!
   When you start the cloning operation, the destination drive will be formatted and all of the data stored on it will be irreversibly erased. Make sure that the disks are empty or do not contain valuable data.

8. Click **Clone**.

5.3 Connecting two Macs

When you want to clone your hard drive to another Mac, the destination Mac must be connected in target disk mode.

[1]This option is not available for a Mac with Apple silicon.

To connect the destination Mac to the source one

1. Turn on both the source and destination Macs.
2. Connect them by using a FireWire or Thunderbolt cable.
3. On the destination Mac, click **Apple menu** > **System Preferences**, click **Startup Disk**, and then click **Target Disk Mode**.

   Once the computer is restarted, a new disk icon appears on the desktop of the source Mac. Since that moment you can work with the hard drive of the destination Mac as an ordinary external drive, including selecting it as a destination drive for the cloning operation.
4. When the cloning operation is complete, eject the destination drive by dragging its icon to the Trash.
5. Turn off the destination Mac, and then disconnect the cable.

6 Protecting family data

6.1 What is family data protection?

Family data protection is a unified cross-platform solution that allows you to track and control the protection status of all computers, smartphones, and tablets sharing the same account. Since users of these devices must be signed in to the same account, usually they are members of the same family. In general, each of them can use this feature, but there is often a family member who is more experienced in technology than the others. So, it's reasonable to make that person responsible for protection of the family data.

To track and control the protection status of your family's devices, use the web-based Online Dashboard, which is accessible from any computer connected to the Internet. With this web application, your family IT administrator can:

- Control the current statuses of all backups and synchronizations on all family devices running Windows, macOS, iOS, and Android.
- Add a new device to the list.
- Manually start any backup on any computer.
- Initiate the first complete backup of an unprotected computer to Acronis Cloud.
- Recover data from any backup located in Acronis Cloud, including backups from PCs, Macs, and devices running iOS and Android.
- Resolve some product-related issues.

6.2 Adding a new device

1. On the device that you want to add, open Online Dashboard at: https://cloud.acronis.com.
2. Sign in with your account.
3. On the **Devices** tab, click **Add device**.
4. Download and install Acronis Cyber Protect Home Office.
5. Start Acronis Cyber Protect Home Office and sign in to the same account.

6.3 Backing up any computer

With the web-based Online Dashboard, you can back up any computer (PC or Mac) that shares the same account.

If a device is not yet protected, you can back up it by using the default settings. Acronis Cyber Protect Home Office will back up the entire contents of the device (for example, an entire PC backup) to Acronis Cloud. These default settings cannot be changed with the web app. If you need to customize the settings, start Acronis Cyber Protect Home Office on this device and configure the backup manually.

To back up any computer

1. Open Online Dashboard at: https://cloud.acronis.com.
2. Sign in with your account.
3. On the **Devices** tab, find the device that you want to back up. If the device is offline, make sure that it is turned on and connected to the Internet.
4. Perform one of the following:
   - If the device was backed up before, click **Back up now**.
     Acronis Cyber Protect Home Office creates a new backup version in accordance with the configured backup scheme.
   - If the device has not yet been backed up, click **Enable backup**, wait until the backup is auto-configured, and then click **Back up now**.
     Acronis Cyber Protect Home Office creates a new full backup and uploads it to Acronis Cloud.

6.4 Recovering data with Online Dashboard

The web-based Online Dashboard allows you to recover data from any online backup uploaded from your family devices, including PCs, Macs, smartphones, and tablets.

To recover data from an online backup

1. Open Online Dashboard at: https://cloud.acronis.com.
2. Sign in with your account.
3. On the **Devices** tab, find the device that is the source of the data that you want to recover. If the device is offline, make sure that it is turned on and connected to the Internet.
4. Click **Recover**.
5. On the left panel, select the backup version by the backup date and time.
6. On the right panel, select the check boxes next to the files and folders that you want to recover.
7. Click **Download**.

7 Archiving data

7.1 What is data archiving?

Data archiving is a tool that allows you to move your big or rarely used files to NAS, an external hard drive, or a USB flash drive. You can also move them to Acronis Cloud. Every time you run this tool, it analyzes the data in the selected folder and suggests moving the found files. You can select the files and folders that you want to archive. After moving to an archive, the local copies of these files will be deleted. The links to the files are stored in a special location called Acronis Drive. You can access the location as an ordinary folder in Finder. Double-clicking a file link will open the file as if it was stored in the local folder. If the file is archived to Acronis Cloud, it will be downloaded back to your computer, first. You can also access and manage it right in Acronis Cloud.

Data archiving has the following main features:

- **Free storage space saving**
  As a rule, storage space of modern high-capacity hard drives is mostly occupied by user data, such as photographs and documents, and not by the operating system or applications. Since most of the data is used occasionally, there is no need to keep them on a local drive. Data archiving helps you free up storage space for frequently used files.
- **Cloud archiving and local archiving**
  You can choose a destination type for your archive: an internal hard drive, external hard drive, NAS, or a USB flash drive. You can also choose Acronis Cloud. Every time you choose Acronis Cloud as a destination, the selected data is stored in the same cloud archive. Local archives are independent from each other and may have different names, destinations, encryption settings, and so on, though you can select an existing archive as a destination instead of creating a new one. The number of local archives is not limited.
- **Easy access of cloud archive from any device**
  When you archive your files to Acronis Cloud, you can access them with Acronis Cyber Protect Home Office, the Acronis Cyber Protect Home Office mobile application, and the Acronis Cloud web application from any device running Windows, macOS, iOS, and Android, including tablets and smartphones.
- **Data protection in the cloud archive**
  Your data stored in Acronis Cloud is protected from corruption or disaster. For example, in case of your local hard drive failure, you can download your files to your new hard drive. Moreover, your data is stored in encrypted state. You can be sure that no one except you can access your data.
- **File sharing**
  When your files are uploaded to Acronis Cloud, you can create public links to share the files with your friends or to post them to forums and social networks.
- **File versions**

For the files that have been changed and uploaded to Acronis Cloud several times, Acronis Cyber Protect Home Office keeps all the modifications in different file versions. You can choose a previous file version and download it to your device.

7.2 What is excluded from archives?

To reduce archive size and eliminate a possibility to corrupt your system, by default Acronis Cyber Protect Home Office excludes the following data from archives:

- pagefile.sys
- swapfile.sys
- Network Trash Folder
- The System Volume Information folder
- The Recycle Bin
- .tib and .tibx files
- .tib.metadata files
- .tmp files
- .~ files

See the full file list in the Knowledge Base article: https://kb.acronis.com/content/58297.

7.3 Cloud archiving vs. Online backup

When you archive your data to Acronis Cloud, it is similar to an online backup, but there are a number of differences.

	Online backup	Cloud archiving
Feature purpose	Data protection from operating system corruption, hardware failures, and loss of separate files.	Cleanup of local storage device and moving data to Acronis Cloud.
Data protection	• Overall protection of all data on a computer, especially an operating system. • Protection of frequently used files.	Protection of rarely used and old files, mostly your personal documents, photographs, and so on.
Source data selection	Manual selection.	Manual selection.
Source data handling	The source data is kept in the original location.	The source data is deleted from the original location. This gives you a guarantee that your data will not get into the wrong hands if your hard drive or laptop is stolen.
Data	The data to back up is changed	The data to archive is changed rarely. The files have

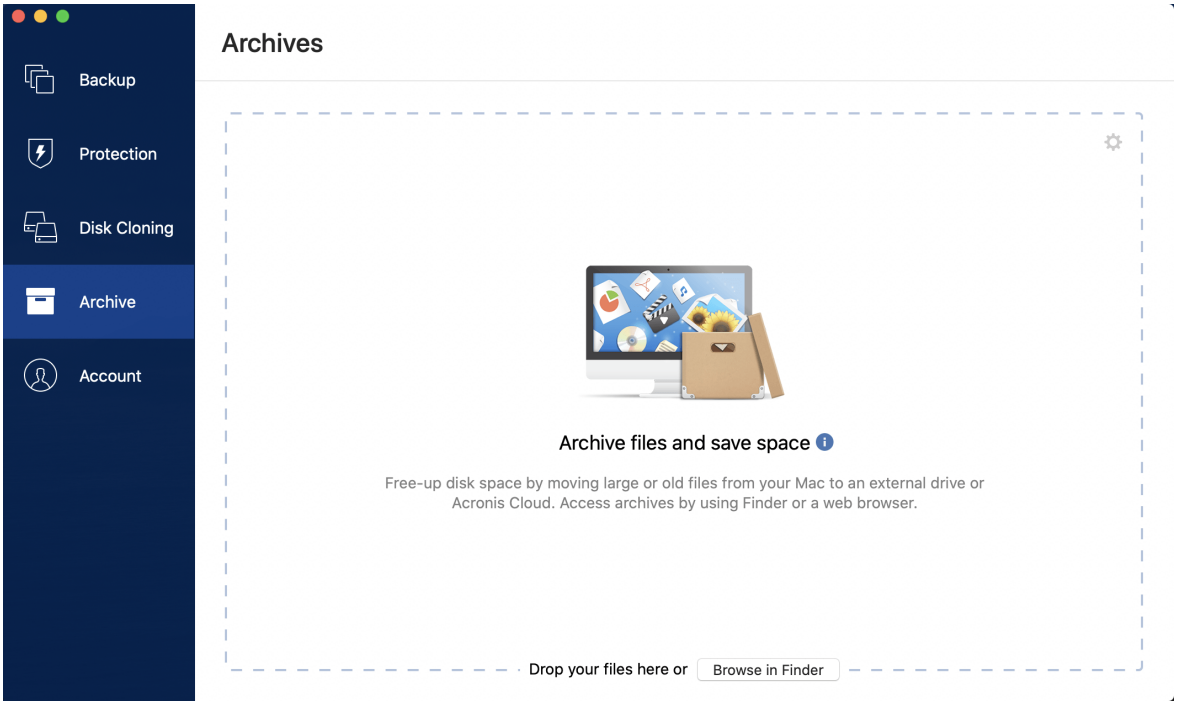
change frequency	frequently. Usually a backup has many versions updated from time to time.	few versions.

7.4 Archiving your data

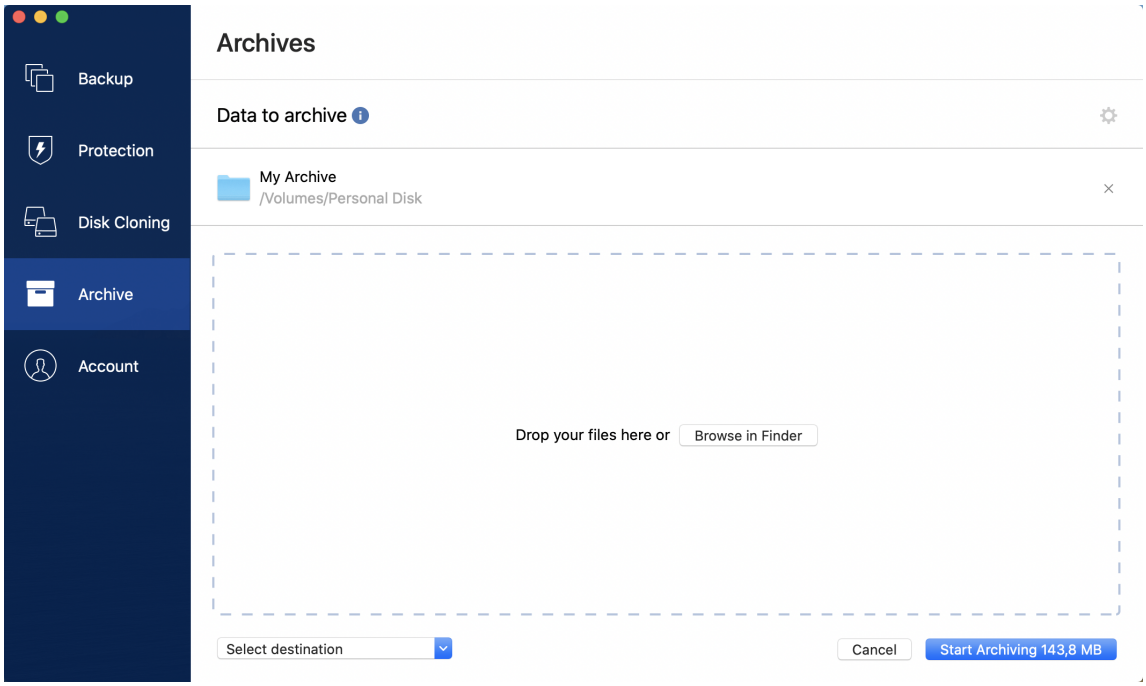
Data archiving helps you free up your storage space by moving your old or rarely used files. Refer to What is data archiving for details.

To archive your data

1. Start Acronis Cyber Protect Home Office, and then go to the **Archive** section.



2. [Optional step] To learn basics of the data archiving feature, view the Getting Started slides.
3. To select files to archive, do one of the following:
   - Drag the files to the Archive screen (for example, from Finder).
   - Click **Browse in Finder**, and then select the files to archive.



4. Click **Select destination**, and then select a destination for the archived files.
5. [Optional step] Click the gear icon to configure additional settings. You can:
   - Protect your archive with a password and encryption at **Settings** —> **Encryption**. Refer to Archive encryption for details.
   - Select a preferred data center and configure the upload speed at **Settings** —> **Advanced**. Refer to Selecting Acronis Cloud data center for details.
6. Click **Start Archiving**.
7. Confirm that you want to move your files to the archive and automatically delete them from your computer.

7.4.1 Network settings for archiving

Data center

When you archive your files to Acronis Cloud, they are uploaded to one of the Acronis data centers located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your archived files are stored in the same data center, by default.

We recommend that you set the data center for an archive manually, when you are in a different country and your default data center is not the closest to your current location. This will significantly increase the data upload rate.

Note
You cannot change the data center after starting the archiving process.

To select a data center

1. When configuring the first archiving process, click the **Settings** icon, and then click **Network**.
2. Select the country that is closest to your current location, and then click **OK**.

Data upload speed

When you archive data to Acronis Cloud, you can change the connection speed used by Acronis Cyber Protect Home Office. Set the connection speed that will allow you to use Internet without annoying slowdowns.

To set up the connection speed, select one of the following options:

- **Maximum**—The data transfer rate is maximum within a system configuration.
- **Custom**—You can specify a maximum value for data upload speed.

7.4.2 Archive encryption

To protect the archived data from unauthorized access, you can encrypt the archive with industry-standard AES (Advanced Encryption Standard) cryptographic algorithm with a 256-bit long key.

Note
You cannot set or change the archive encryption option for a pre-existing archive.

To encrypt an archive

1. When configuring the first archiving process, click the **Settings** icon, and then click **Encryption**.
2. Enter the password for the archive into the corresponding field, and then click **OK**.
   We recommend that you use a password longer than seven symbols and containing both letters (in upper and lower cases preferably) and numbers to make it more difficult to guess.
   A password cannot be retrieved. Please memorize the password that you specify for an archive protection.

7.5 Accessing your archived files

When your files are successfully archived, you can access them in:

- **Finder**
  Open Finder, and then click **Acronis Drive** under **Favorites**.
  You can work with the files in read-only mode. To modify a file, copy it to a different folder, first.
- **Acronis Cloud** (applicable to the cloud archive only)
  1. Open Acronis Cyber Protect Home Office, click **Archives**, and then click **Open in web browser**.
  2. On the **Archive** tab of the Acronis Cloud website, select the required archive with a check mark.
  3. Click **Download** on the right sidebar.
  4. The selected data will be copied to the default downloads folder.

8 Sharing data

You can share files and folders stored in backups and archives stored in Acronis Cloud.

1. On the Acronis Cyber Protect Home Office sidebar, click **Account**.
2. In the **Acronis Cloud Storage** section, click **Browse my data**.
   You are redirected to the Acronis Cloud browser page.
3. Depending on what you want to share, do the following:
   - If you want to share a file or folder from a backup, on the left sidebar, click **BACKUPS**. Select the required file or folder with a check mark.
   - If you want to share a file or folder from an archive, on the left sidebar, click **ARCHIVES**. Select the required file or folder with a check mark.
4. On the right sidebar, click **Share link**.
5. [Optional] You can configure the sharing options. To do that, in the link window, click **Link settings**. You can apply a password, set the expiration date, and limit the amount of downloads.
6. In the link window, click **Copy link** and close it.

You can now share this link. To see the shared files, on the left sidebar, click **SHARING**. You can select any file here, and on the right sidebar copy its link, configure the link settings, or delete it.

9 Protection

Acronis Cyber Protect Home Office provides the following types of protection:

- Active Protection runs constantly in the background to protect your machines in real time while you work as usual.
- Antivirus Scans run on-demand to perform in-depth search for malicious software throughout the whole system.
- Vulnerability assessment is a daily scan that runs in the background, detects vulnerabilities in your system and apps, and then assesses their severity.

Note
You can turn the protection on or off in the Acronis Cyber Protect Home Office UI only. You cannot stop the process manually through Activity Monitor or any other external tool.

9.1 The Protection dashboard

The Protection dashboard contains statistical data, provides control over the protection status, and access to the protection setting.

To access the Protection dashboard, click **Protection** on Acronis Cyber Protect Home Office sidebar.

On the **Overview** tab of the dashboard, you can:

- View statistics about the active protection status.
- View the number of detected issues and quarantined items.
- View the latest report of the **Antivirus scan**.
- View the next scheduled scan time.
- Manually run full **Antivirus scan**. To do this, click **Run full scan**.
- View the latest report of the detected vulnerabilities, and run a new scan from it.
- Stop the entire protection for a predefined period of time (30 minutes, 1 hour, 4 hours, until restart). To do this, click **Turn Off Protection** and choose the period.

  Note
  By pausing the protection, you deactivate Active Protection. Scheduled on-demand scans will not start.

On the **Activity** tab of the dashboard, you can view a log of the changes that you applied to your protection status and settings.

9.2 Active Protection

To protect your computer from malicious software, Acronis Cyber Protect Home Office uses the Acronis Active Protection technology.

Active Protection constantly checks your computer while you continue working as usual. In addition to your files, Acronis Active Protection protects the Acronis Cyber Protect Home Office application files and your backups.

Active protection consists of two protection levels that you can enable independently from each other:

- Anti-ransomware Protection
- Real-time Protection

9.2.1 Anti-ransomware Protection

Ransomware encrypts files and demands a ransom for the encryption key.

When the **Anti-ransomware Protection** service is on, it monitors in real time the processes running on your computer. When it detects a third-party process that tries to encrypt your files, the service informs you about it and asks if you want to allow the process to continue or to block the process.

To allow the process to continue the activity, click **Trust**. If you are not sure if the process is safe and legal, we recommend that you click **Quarantine.** After this, the process will be added to **Quarantine** and blocked from any activities.

Recovering your files after blocking a process

After blocking a process, we recommend that you check if your files have been encrypted or corrupted in any way. If they are, click **Recover modified files**. Acronis Cyber Protect Home Office will search the following locations for the latest file versions to recover.

- Temporary file copies that were preliminarily created during the process verification
- Local backups
- Cloud backups

If Acronis Cyber Protect Home Office finds a good temporary copy, the file is restored from that copy. If temporary file copies are not suitable for restore, Acronis Cyber Protect Home Office searches for backup copies, compares the creation dates of the copies found in both locations, and restores your file from the latest available non-corrupt copy.

Note
Acronis Cyber Protect Home Office does not support file recovery from password-protected backups.

9.2.2 Real-time Protection

When **Real-time Protection** is enabled, it constantly checks the files you interact with to protect your machine from suspicious activity, viruses, and other malicious threats in real time.

Real-time Protection has two modes of operation:

- **Smart on-access**—all system activities are monitored, and the files are scanned once you access them.
- **On execution**—only executable files are scanned as they are launched to make sure that they will not damage your machine.

You can configure Real-time protection what to do with blocked files:

- **Block and quarantine**—The process suspected of malware activity will be blocked, and the file will be moved to the quarantine folder.
- **Block and notify**—The process suspected of malware activity will be blocked, and you will get a notification.

You can view the results in the **Activities** list.

9.2.3 Configuring Active Protection

To configure Anti-ransomware Protection

1. Click **Protection** on the Acronis Cyber Protect Home Office side bar, then click **Settings**.
2. Go to the **Active Protection** tab and enable **Anti-ransomware Protection**.

When enabled, Anti-ransomware Protection protects your computer from potentially harmful applications and processes that run in the background.

To configure Real-time Protection

1. Click **Protection** on the Acronis Cyber Protect Home Office side bar, then click **Settings**.
2. Go to the **Active Protection** tab and enable **Real-time Protection**.
   When enabled, Real-time Protection checks for malware all the files you interact with.
3. Select when the files should be checked.
   - **Smart on-access**—All system activities are monitored, and the files are scanned once you access them.
   - **On execution**—Only executable files are scanned as they are launched to make sure that they will not damage your machine.
4. Select what to do with detected objects.
   - **Block and notify**—The process suspected of malware activity will be blocked, and you will get a notification.
   - **Block and quarantine**—The process suspected of malware activity will be blocked, and the executable file will be moved to the quarantine folder.
5. Click **OK**.

9.3 Antivirus Scans

Antivirus scan is one of the components of Acronis Cyber Protect Home Office Antivirus and Anti-malware Protection. It protects your computer by checking for malware on demand – manually or at predefined intervals that you can configure.

You can select between two types of scans.

- **Full** scan checks the entire machine for viruses. Full scan will detect malware by examining all files and processes (or a subset of files and processes), except for excluded files or folders that you defined in the excludes lists.
- **Quick** scan checks only specific files and folders. Quick scan will detect malware by examining specific folders which are considered the most likely virus storages.

You can also choose what to scan: archive files, external drives, or only new and changed files.

Sometimes, the system might be shut down before the Antivirus scan is completed. For such cases, you can configure Acronis Cyber Protect Home Office to resume the scan when the system starts again. Moreover, you can configure Acronis Cyber Protect Home Office to prevent your computer from shutting down if a scan operation is running.

By default, in case of a CPU overload, the priority of antivirus scans is decreased to let other applications perform properly in. This slows down the scanning when the CPU is overloaded. You can speed up the scanning process by disabling this option.

You can view the **Antivirus scan** results in the **Scan details report**.

9.3.1 Configuring Antivirus Scans

1. Click **Protection** on the Acronis Cyber Protect Home Office side bar, then click **Settings**.
2. Go to the **Antivirus** tab and apply the required settings.
3. To configure scan type, on the **Schedule** tab, select the required check box.
   - **Full**—This option is set by default. Acronis Cyber Protect Home Office will check the entire Mac.
   - **Quick**—Acronis Cyber Protect Home Office will check only the specific folders that are considered the most likely storages of threats.
4. To schedule antivirus scans, on the **Schedule** tab, select the required check boxes to configure the time when the scanning process shall start.
   - **Do not schedule**—The scan run is not planned for a specific time.
   - **Daily**—The scan will be run every day at a specified time. Set the time.
   - **Weekly**—The scan will be run on a specified day of week. Set the day of week and time.
   - **Monthly**—The scan will be run on a specified day of month.
   - **At system startup**—The scan will be run at each start of your operating system.
5. To configure an action on detection, on the **Options** tab, select the required check boxes.
   - **Quarantine**—This option is set by default. When Acronis Cyber Protect Home Office detects a potential malware threat, it stops the process and moves the suspicious file to the quarantine folder.
   - **Notify only**—When a suspicious process is detected, you will get a notification about the potential malware threat.
6. To configure what to scan, on the **Options** tab, select the required check boxes.
   - **Scan archive files**
   - **Scan external drives**

- **Scan network shares and NAS**
- **Scan only new and changes files**

7. To configure the system behavior during Antivirus scans, select the required check boxes.
   - **Prevent the sleep or hibernate mode**—Your computer will not shut down unless the scan is performed.
   - **Run missed tasks at the startup**—If some of the tasks were not completed before the system shut down, scanning process is resumed when the system starts again.
   - **Give priority to other applications**—In case of a CPU overload, the antivirus scan priority can be decreased to let other applications perform properly. By default, the check box is selected, and in this case, scanning will take more time.
8. After configuring the Antivirus scan options, click **OK** to save your changes.

You can view the Antivirus scan results in **Scan details report**.

9.4 Vulnerability assessment

Vulnerability assessment is one of the components of Acronis Cyber Protect Home Office Antivirus and Anti-malware Protection. It is a daily scan that runs in the background, detects vulnerabilities in your system and apps, and then assesses their severity. You can also run it manually when needed.

Note
Vulnerability assessment requires a stable internet connection.

To view the vulnerabilities:

1. On the left sidebar, click **PROTECTION**.
2. On the **Overview** tab, under **Vulnerability assessment**, click **Detected vulnerabilities**. The report is displayed.
3. To run a new scan, click **Run Scan**.
4. [optional] To view the detailed information on a vulnerability in Acronis Cyber Protect Home Office, click the arrow next to its name. The **Detailed information** window opens with the vulnerability details, like the affected product version.
5. [optional] To view more information on a vulnerability:
   - In the report, click the **i** icon next to the vulnerability name.
   - In the **Detailed information** window, click **More information**.

   A webpage will be displayed with the detailed description of the vulnerability.
6. To resolve the detected issues, install the latest updates of the affected applications. Then, scan again to ensure that the vulnerabilities are fixed. If they persist, it means that some apps might still put your system at risk. To protect your data fully, back up your entire machine and enable Anti-malware Protection.

To configure the vulnerability assessment:

1. On the left sidebar, click **PROTECTION**, then click **Settings**.
2. Go to the **Vulnerability assessment** tab, and select or clear the check box to enable or disable the vulnerability scan.

Index