

Acronis



Acronis True Image 2018

USER GUIDE

Table of contents

1	Introduction	4
1.1	What is Acronis® True Image™?	4
1.2	System requirements	4
1.3	Install, update, or remove Acronis True Image 2018	5
1.4	Activating Acronis True Image 2018	6
1.5	Trial version information	8
1.6	Acronis Customer Experience Program	8
1.7	Sending feedback to Acronis	9
1.8	Application preferences	10
1.9	Keyboard shortcuts	10
1.10	Technical Support	11
2	Backup	12
2.1	Basic concepts	12
2.2	What you can and cannot back up	13
2.3	Backing up to local or network storage	14
2.4	Backing up to Acronis Cloud	15
2.5	Notarized backup	17
2.5.1	Using Blockchain technology	18
2.5.2	Verifying file authenticity	19
2.5.3	Manual verification of a file's authenticity	20
2.6	Backing up mobile devices	20
2.6.1	Acronis Mobile	21
2.6.2	Local destination of mobile backups	22
2.7	Backing up a Facebook account	23
2.8	Backing up an Instagram account	23
2.9	Scheduling	25
2.10	Backup encryption	26
2.11	Backup retention rules	26
2.12	Excluding items from backups	27
2.13	Connection settings	29
2.14	Network settings for backup	30
2.15	Backup activity and statistics	31
2.16	Laptop power settings	32
2.17	Notifications	32
2.18	What is Acronis Cloud?	33
2.18.1	Creating an Acronis account	34
2.18.2	Subscription to Acronis Cloud	34
2.19	Parallels Desktop support	34
2.20	Backup list icons	36

2.21	Sorting backups in the list.....	37
3	Creating bootable rescue media	38
4	Recovery	39
4.1	When do I recover my Mac?.....	39
4.2	Recovering your Mac	39
4.2.1	FAQ about Boot Camp partition.....	41
4.3	Recovering your files	41
4.4	Recovering cloud data from any device	42
4.5	Recovering your Facebook account.....	44
4.6	Recovering your Instagram account	44
4.7	Searching backup content	45
4.8	Network connection transfer rate	45
5	Protecting family data.....	46
5.1	What is family data protection?	46
5.2	Adding a new device	46
5.3	Backing up any computer	46
5.4	Recovering data with Online Dashboard.....	47
6	Archiving data.....	48
6.1	What is data archiving?	48
6.2	What is excluded from archives?.....	49
6.3	Cloud archiving vs. Online backup.....	49
6.4	Archiving your data.....	50
6.4.1	Network settings for archiving	51
6.4.2	Archive encryption	52
6.5	Accessing your archived files	52
7	Tools	53
7.1	Acronis Active Protection	53
7.1.1	Protecting your data from ransomware.....	54
7.1.2	Acronis Active Protection settings	55

1 Introduction

In this section

What is Acronis® True Image™?	4
System requirements	4
Install, update, or remove Acronis True Image 2018.....	5
Activating Acronis True Image 2018	6
Trial version information.....	8
Acronis Customer Experience Program	8
Sending feedback to Acronis.....	9
Application preferences.....	10
Keyboard shortcuts	10
Technical Support	11

1.1 What is Acronis® True Image™?

Acronis True Image 2018 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 (p. 14) and Backing up to Acronis Cloud (p. 15) for details.

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 bootable rescue media (p. 38) for details.

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

Key features:

- Backup of selected disks or entire Mac contents to local or network storage (p. 14) or to Acronis Cloud (p. 15)
- Backup of selected files and folders to local or network storage (p. 14) or to Acronis Cloud (p. 15)
- Data archiving (p. 48)
- Family data protection (p. 46)
- Creating bootable rescue media (p. 38)
- Mac OS X recovery in the bootable media environment (p. 39)
- Recovery of specific files and folders under Mac OS X (p. 41)

1.2 System requirements

Supported operating systems:

- OS X Yosemite 10.10.5

- OS X El Capitan 10.11.6+
- macOS Sierra 10.12
- macOS High Sierra 10.13

Supported file systems:

- Apple File System (APFS)
- Mac OS Extended format (case-insensitive)
- FAT32
- exFAT
- NTFS (read-only)

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 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
- Network share, NAS
- Acronis Cloud

General requirements:

- You need to have administrator privileges to run Acronis True Image 2018.

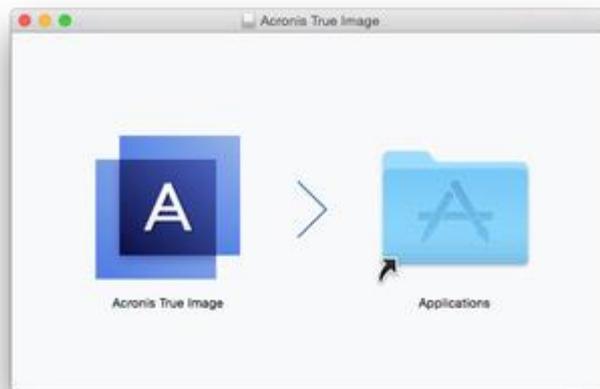
1.3 Install, update, or remove Acronis True Image 2018

Installation

To install Acronis True Image 2018:

1. Download the Acronis True Image 2018 setup file from the Acronis website:
 - To purchase the full version, go to:
www.acronis.com/redirector/products/timac2018/getfullversion/.
 - To try the free trial version, go to:
www.acronis.com/redirector/products/timac2018/getfreetrial/.
2. Read and accept the terms of the license agreement and the Acronis Customer Experience Program.

3. Double-click the Acronis True Image 2018 setup file (the file has a .dmg extension).



4. Drag the Acronis True Image 2018 icon to the Applications folder.

When you start Acronis True Image 2018 for the first time, sign in to your Acronis account. The product will be automatically activated. You can skip this step. In this case, enter your serial number, and then click **Activate**. Refer to *Activating Acronis True Image 2018* (p. 6) for details.

Update

When an update for Acronis True Image 2018 is available from the Acronis website, you can download it, and then install it over your version of Acronis True Image 2018. All your backups and settings will be kept.

To turn on an automatic check:

- In the **Acronis True Image** menu, click **Preferences**, and then select the **Automatically check for updates at startup** check box.

To check for updates manually:

- In the **Acronis True Image** menu, click **Check for Updates**.

Uninstallation

To remove Acronis True Image 2018 from your Mac:

1. Open the Finder, and then click **Applications**.
2. Find Acronis True Image 2018 in the list, and then drag it to the Trash.

1.4 Activating Acronis True Image 2018

To use Acronis True Image 2018, 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.

Activating Acronis True Image 2018

You can activate Acronis True Image 2018 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 True Image 2018 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 True Image 2018 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 True Image 2018.
2. On the sidebar, click **Account**, and then click **Activate offline**.
3. In the Acronis True Image 2018 Activation window, perform 3 simple steps:
 1. 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.
 2. On another computer which has the Internet connection, go to <http://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.
 3. 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>.

"Too many activations" issue

Possible reasons for the issue:

- **You exceed the maximum number of computers with installed Acronis True Image 2018.**

For example, you have one license or a serial number for one computer and you install Acronis True Image 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 to your new computer from another one on which the product is already activated. To do this, select the computer from which you want to move the license. Note that Acronis True Image will be deactivated on that computer.
- **You reinstall macOS or change hardware of your computer.**

For example, you might upgrade motherboard or processor in your computer. Activation is lost, because Acronis True Image sees your computer as a new one.

Solution:

To reactivate Acronis True Image on your computer, choose from the list the same computer by its old name.

Managing your subscription licenses manually

If you use the subscription-based version of Acronis True Image 2018, 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 True Image 2018, and then click **Manage**.

1.5 Trial version information

If you want first to try and evaluate Acronis True Image 2018, you can install the free, 30-day trial version of the product. The trial version is fully functional. 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 True Image 2018.

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 True Image 2018.

Acronis Cloud

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.

Installing the trial version

To start using the trial version, install the product, and then click **Start Trial**. Refer to Install, update or remove Acronis True Image 2018 (p. 5) for details.

Upgrading to the full version

To upgrade to the full version of the product:

1. Purchase the full version at the Acronis website:
www.acronis.com/redirector/products/atimac2018/getfullversion/.
2. Open Acronis True Image 2018.
3. On the menu bar, click **Acronis True Image 2018**, and then click **Enter Serial Number**.
4. Insert the full serial number in the appropriate box, and then click **Proceed**.

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 make a decision:

1. In the **Acronis True Image** 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.

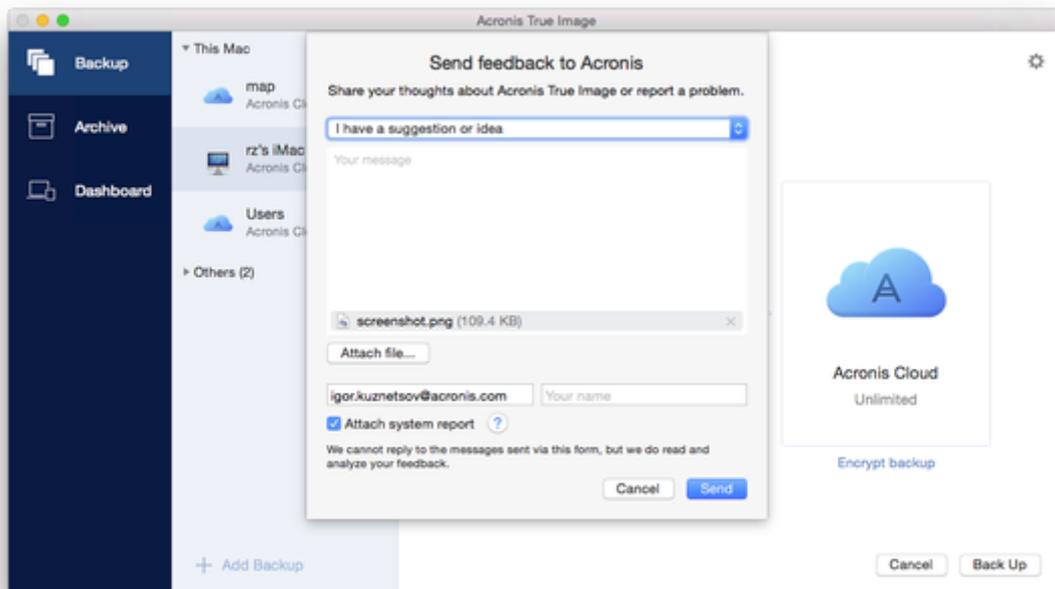
1.7 Sending feedback to Acronis

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 True Image 2018 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.

We do not reply to all feedback messages. If you need assistance with Acronis True Image 2018, contact Technical Support (p. 11).

To send a feedback to Acronis:

1. In the **Acronis True Image 2018** 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 True Image 2018 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, OS X version, system log, event log of Acronis True Image 2018, 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 True Image 2018 stopped responding.
7. Click **Send**.

1.8 Application preferences

The Preferences window contains general settings of Acronis True Image 2018. To open it:

1. Open Acronis True Image 2018.
2. In the Acronis True Image menu, click **Preferences**.

The following settings are available:

- **Do not back up when working on battery power**
Refer to Laptop power settings (p. 32) for details.
- **Automatically check for updates at startup**
Refer to Install, update, or remove Acronis True Image 2018 (p. 5) for details.
- **Participate in the Acronis Customer Experience Program**
Refer to Acronis Customer Experience Program (p. 8) for details.
- **Show notifications in Notification Center**
Refer to Notifications (p. 32) for details.

1.9 Keyboard shortcuts

In Acronis True Image 2018, 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 True Image 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 True Image 2018:

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 Acronis account
Shift + Command + O	Sign out from Acronis account
Command + N	Create new backup
Command + 1	Open the Backup section
Command + 2	Open the Archive section
Command + 3	Open the Active Protection section
Command + 4	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
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 Technical Support

Maintenance and Support Program

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

Product Updates

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** (<http://kb.acronis.com/content/4834>) and **Acronis Website User Guide** (<http://kb.acronis.com/content/8128>).

2 Backup

In this section

Basic concepts.....	12
What you can and cannot back up.....	13
Backing up to local or network storage	14
Backing up to Acronis Cloud	15
Notarized backup.....	17
Backing up mobile devices.....	20
Backing up a Facebook account.....	23
Backing up an Instagram account	23
Scheduling.....	25
Backup encryption	26
Backup retention rules.....	26
Excluding items from backups	27
Connection settings	29
Network settings for backup.....	30
Backup activity and statistics	31
Laptop power settings	32
Notifications.....	32
What is Acronis Cloud?.....	33
Parallels Desktop support.....	34
Backup list icons.....	36
Sorting backups in the list.....	37

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 (p. 39) 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 (p. 14) and Backing up to Acronis Cloud (p. 15) for details.
- To recover specific files and folders (p. 41) 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 True Image 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 True Image 2018 saves backup data in the proprietary .tib format, by using compression. The data from .tib file backups can be recovered only through Acronis True Image 2018.

When you back up your Mac to Acronis Cloud (p. 33), Acronis True Image 2018 saves your data "as is". You can recover the data in the product or via the Acronis Cloud web application (p. 33) 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 (p. 25) to run on a regular basis.

Backup retention rules

Every time you run a backup operation, manually or on a schedule, Acronis True Image 2018 creates a new backup version in the backup location. To delete obsolete backup versions automatically, you can set the backup retention rules. Refer to Backup retention rules (p. 26) 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 drives	+	+	+	+	+	+	-	-
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

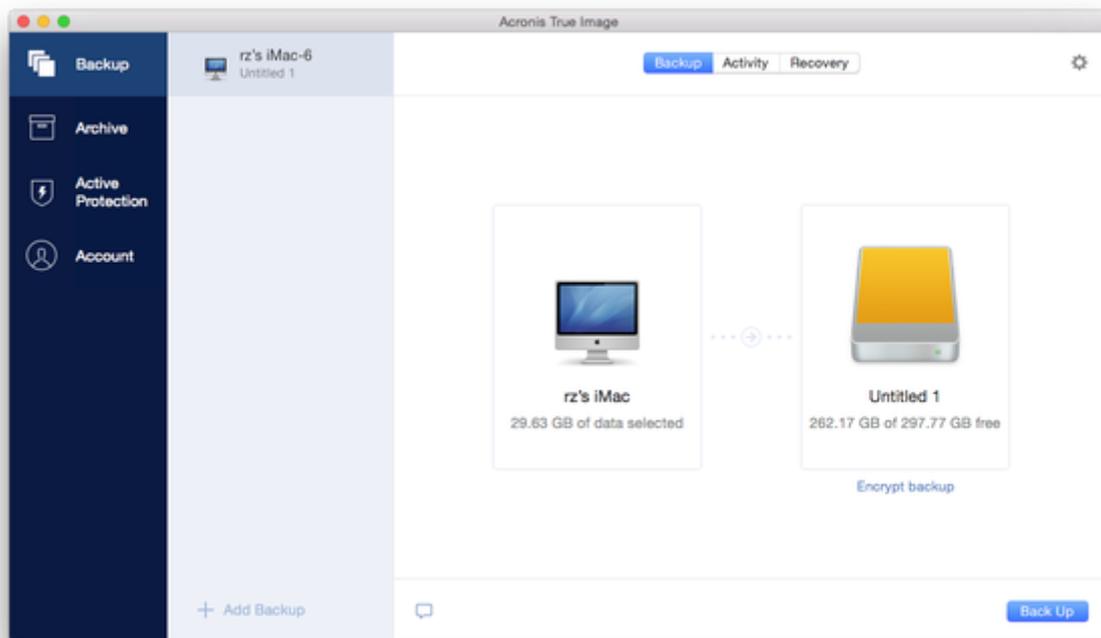
To back up your data to local or network storage:

1. Open Acronis True Image 2018.
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, and then select what you want to back up:
 - **Entire Mac**
When you select this option, Acronis True Image 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 (p. 20) for details.
 - **Social network**
Refer to Backing up a Facebook account (p. 23) or Backing up an Instagram account (p. 23) for details.
 - **Files to notarize**
Refer to Notarized backup (p. 17) for details.

- NAS device (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 (p. 27) for details.
 - Configure the backup schedule at **Settings** —> **Schedule**. Refer to Scheduling (p. 25) for details.
 - Set the backup retention rules at **Settings** —> **Cleanup**. Refer to Backup retention rules (p. 26) for details.
 - Protect your backup with a password and encryption at **Settings** —> **Encryption**. Refer to Backup encryption (p. 26) 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 an Acronis True Image backup, you must have an Acronis bootable media. If you do not have one, please create it. Refer to Creating bootable rescue media (p. 38) for details.

2.4 Backing up to Acronis Cloud

To start using Acronis Cloud:

- Create an Acronis account (p. 34), if you do not have one.
- Subscribe to the Acronis Cloud service (p. 34).

To back up your Mac to Acronis Cloud:

1. Open Acronis True Image 2018.
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 deleted from the backup storage.*

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

- **Entire Mac**

When you select this option, Acronis True Image 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 (p. 20) for details.

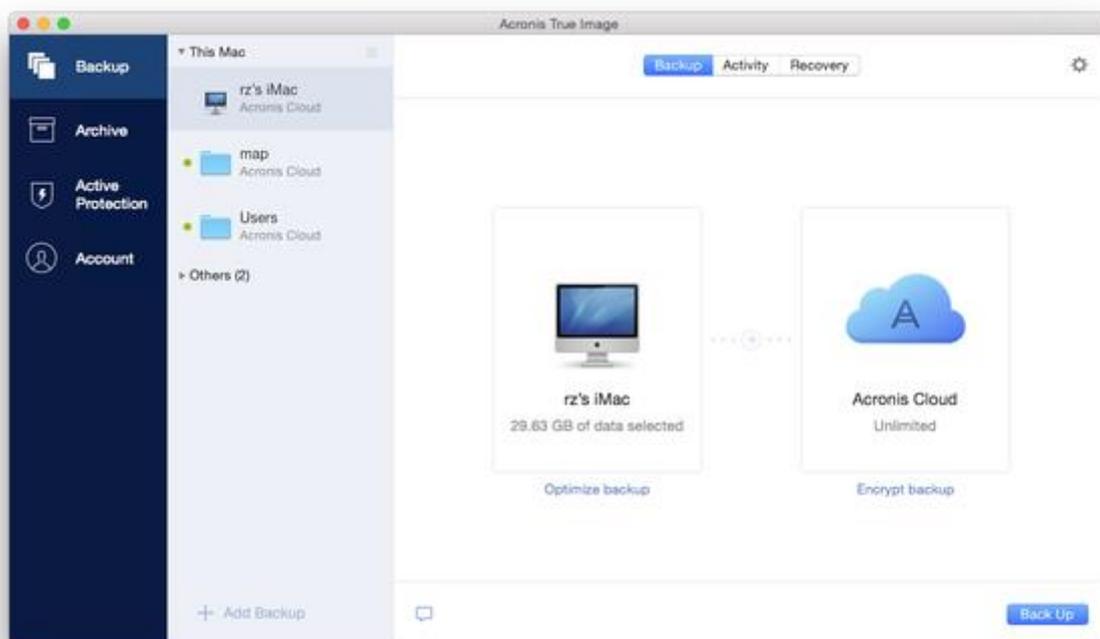
- **Social network**

Refer to Backing up a Facebook account (p. 23) or Backing up an Instagram account (p. 23) for details.

- **Files to notarize**

Refer to Notarized backup (p. 17) 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 (p. 34) 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 (p. 27) for details.
 - Exclude files and folders manually at **Settings** → **Exclusions**. Refer to Excluding items from backups (p. 27) for details.
 - Configure the backup schedule at **Settings** → **Schedule**. Refer to Scheduling (p. 25) for details.
 - Set the backup retention rules at **Settings** → **Cleanup**. Refer to Backup retention rules (p. 26) for details.
 - Protect your backup with a password and encryption at **Settings** → **Encryption**. Refer to Backup encryption (p. 26) for details.
 - Select a preferred data center and configure the upload speed at **Settings** → **Network**. Refer to Network settings for backup (p. 30) for details.
6. After you have configured all settings and you are ready to start a backup, click **Back Up**.

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 an Acronis True Image backup, you must have an Acronis bootable media. If you do not have one, please create it. Refer to Creating bootable rescue media (p. 38) for details.

2.5 Notarized backup

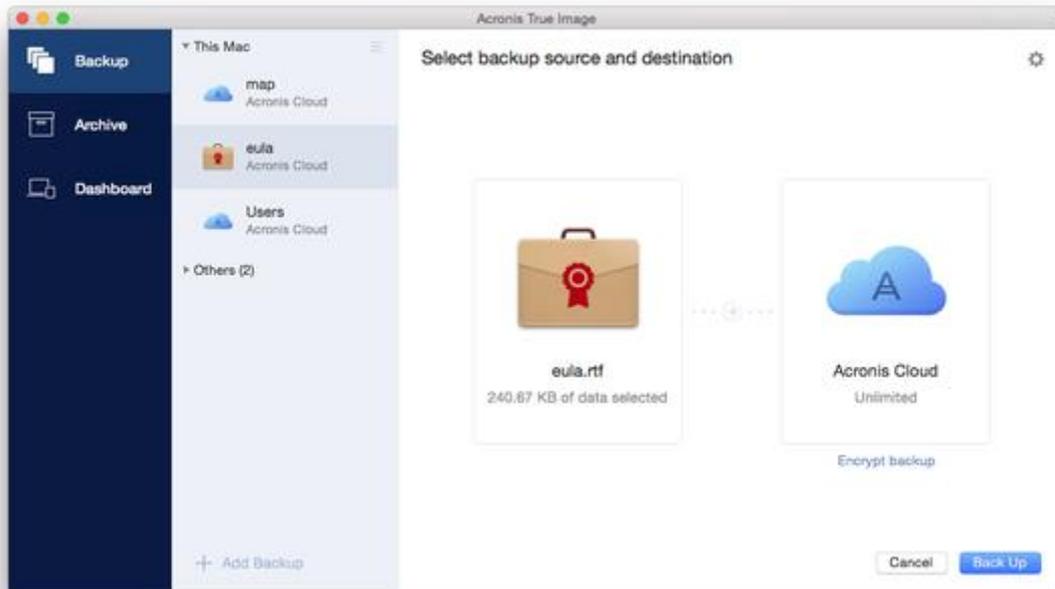
By using Blockchain technology, Acronis True Image 2018 can protect your files from unauthorized modification. This gives you a guarantee that you can recover your data from the same file that was backed up. We recommend that you use this type of backup to protect your legal document files or any other files that require proved authenticity. Refer to Using Blockchain technology (p. 18) for details.

To create a notarized backup of your files and folders:

1. Open Acronis True Image 2018.
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 **Notarized backup**, 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 (p. 27) 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 (p. 27) for details.
 - Configure the backup schedule at **Settings** —> **Schedule**. Refer to Scheduling (p. 25) for details.
 - Set the backup retention rules at **Settings** —> **Cleanup**. Refer to Backup retention rules (p. 26) for details.
 - Protect your backup with a password and encryption at **Settings** —> **Encryption**. Refer to Backup encryption (p. 26) for details.
 - Select a preferred data center and configure the upload speed at **Settings** —> **Network**. Refer to Network settings for backup (p. 30) for details.
6. After you have configured all settings and you are ready to start a backup, click **Back Up**.

2.5.1 Using Blockchain technology

Acronis True Image 2018 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_\(database\)](https://en.wikipedia.org/wiki/Blockchain_(database)).

How Acronis True Image 2018 uses the Blockchain technology

To protect your files from unauthorized modification, Acronis True Image 2018 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 True Image 2018 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 (p. 19). 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 (p. 20) for details.

2.5.2 Verifying file authenticity

By using Blockchain technology, Acronis True Image 2018 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:

1. Open Acronis True Image 2018.
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, click **Recover files**.
5. Depending on the backup location:

- For a local backup, 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 True Image 2018 will check the file authenticity.
- For a cloud backup, the Acronis Cloud web application will open. On the **Files** tab, browse to the required file, point to the file name, and then click the **View certificate** icon or the **Verify** icon. See the commands description above.

If a notarized backup is stored on Acronis Cloud, you can also verify a backed-up file's authenticity in the Acronis Cloud web application.

To verify a file's authenticity on Acronis Cloud:

1. Go to [https://www.acronis.com/my/online-backup/webstore/](https://www.acronis.com/my/online-backup/webrestore/), and then log in to your Acronis account.
2. On the **Files** tab, browse to the required file, point to the file name, and then click the **View certificate** icon or the **Verify** icon. See the commands description above.

2.5.3 Manual verification of a file's authenticity

The easiest way to verify a file's authenticity is to use the **Verify** command in Acronis True Image 2018 or in the Acronis Cloud web application. Refer to Verifying file authenticity (p. 19) 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 (p. 19) 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>.

2.6 Backing up mobile devices

If you have an iOS or Android smartphone or tablet, you can use Acronis True Image 2018 to protect your mobile data such as photos, video files, contacts, and calendars. Refer to Acronis Mobile (p. 21) 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, 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:
 1. Start Acronis True Image 2017, or later version.
 2. On the sidebar, click **Backup**, and then click **Add Backup**.
 3. 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:
 1. Start Acronis Mobile.
 2. Select computer as a backup destination.
 3. 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.
 4. Select the data categories that you want to back up.
 5. [optional step] Turn on the **Encrypt backup** setting to encrypt the backup and protect it with a password. If you do not want the app to ask you for the password when you access the backup on your mobile device, turn on the **Remember password** setting. You can turn it off later in Settings.
 6. Tap **Back up now**.
 7. Allow Acronis Mobile to access to your personal data.

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 both Acronis True Image 2018 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**.

When you change a mobile backup destination from local storage to Acronis Cloud, the connection between the mobile device and the computer is lost, and Acronis True Image stops associating the mobile backup in the list with the mobile device. Then, if you want to change the destination back to local storage, you will need to restore this connection. The connection may also be lost because of an error. To restore it, select the mobile backup in the backup list of Acronis True Image, click **Reconnect**, and then scan the QR code with your mobile device. After that, the backup will continue normally with the same settings.

2.6.1 Acronis Mobile

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

Acronis Mobile allows you to back up your data to Acronis Cloud, to local storage on your computer, or to an NAS device, 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 8.0 and later (iPhone, iPad, iPod)
- Android 4.1 and later (mobile phones and tablets)

Key features

Acronis Mobile allows you to:

- Back up your personal data, including:
 - Photos
 - Videos
 - Photos and videos located in iCloud (iOS only)
 - Contacts
 - Calendars
 - Messages (Android only)
 - Reminders (iOS only)
- Choose the following locations as a backup destination:
 - Acronis Cloud
 - Local storage on your computer
 - NAS
- 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://itunes.apple.com/us/app/acronis-true-image-cloud/id978342143>
- Acronis Mobile for Android devices:
<https://play.google.com/store/apps/details?id=com.acronis.acronistrueimage>

2.6.2 Local destination of mobile backups

When you back up your mobile data to a computer, Acronis True Image stores the backups in the default folder `/Library/Application Support/Acronis Mobile Backup Data/acronis-local-data/`. When you change the destination, the `acronis-local-data` folder is moved to the location that you select. During this operation, the current mobile backups are paused and will automatically resume when the operation completes. All new mobile data will be backed up to the new destination.

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

To change a 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 destination to the initial one, click **Reset to default**.

2.7 Backing up a Facebook account

Acronis True Image 2018 allows you to protect your entire Facebook account from losing your photos, posts, profile information, and other data and activities. The copy of your account is uploaded to secure Acronis Cloud and is accessible from any device. After uploading the data, you can browse it and recover a specific item or the entire account.

Data that you can back up:

- Profile
Basic information, including name, email, birth date, gender, website.
- Timeline
Your posts and posts of other people on your wall.
- Photos and videos
Your albums, as well as photos and videos you are tagged in.
- Events
Description of events that you are invited to visit.
- Liked pages
Links to the pages that you liked, with page names and pictures.

To back up your Facebook account to Acronis Cloud:

1. Open Online Dashboard by doing one of the following:
 - Follow the link: <https://cloud.acronis.com>.
 - On the sidebar of Acronis True Image 2018, click **Backup**, click **Add Backup**, click the **Backup source** area, and then select **Social network**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, click **Add**, and then choose **Facebook**.
4. Click **Back up Facebook**.
5. Log in to your Facebook account.
6. Click **OK** to allow Acronis True Image 2018 to access information from your Facebook account. The information will only be used for backup purposes.
7. Configure the backup by selecting the items that you want to back up and setting a schedule for the backup. You can also encrypt the backup and protect it with a password (available in Acronis True Image 2018 and later). When done, click **Apply**.
8. To start the backup, click **Run now**.

2.8 Backing up an Instagram account

With Acronis True Image 2018, you can protect your Instagram account from losing your photos and videos by backing up them to secure Acronis Cloud. Your posts are stored in the same order they were published and contain the photo or video, its description, tags, and the number of comments

and likes. After uploading to Acronis Cloud, all the content is available from any device any time. You can browse it, view, and download specific posts or all of them at once.

Note: Instagram does not support recovery of posts or profile information to the Instagram application. You can only download them.

Data that you can back up:

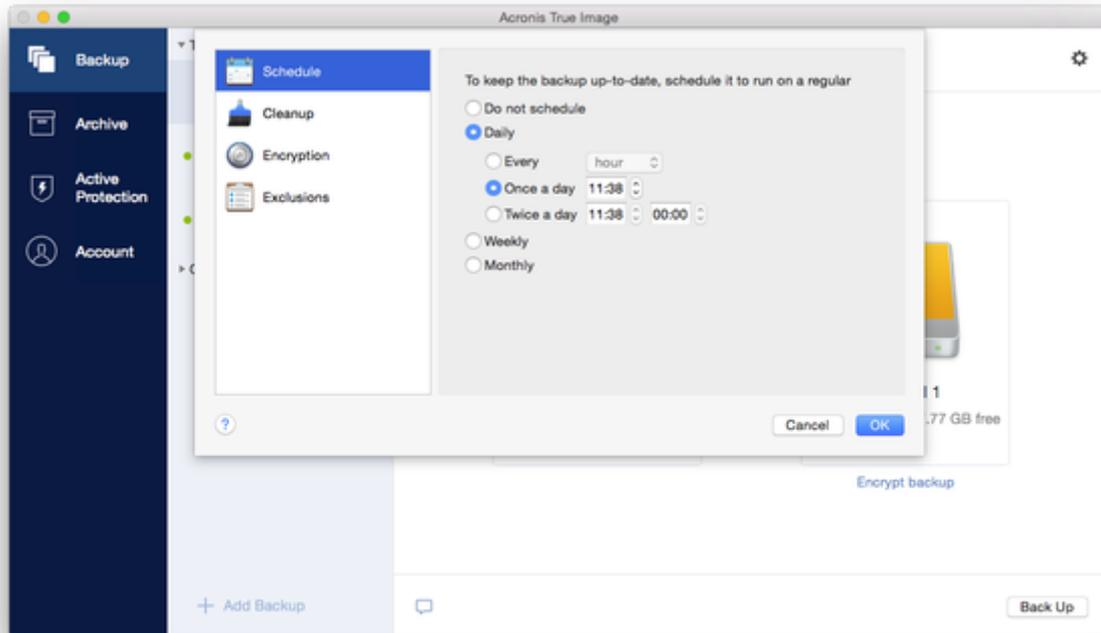
- **Profile**
Basic information, including user name, website, biography.
- **Posts**
The photos and videos you post in your account, descriptions, hashtags, and the number of comments and likes.

To back up your Instagram account to Acronis Cloud:

1. Open Online Dashboard by doing one of the following:
 - Follow the link: <https://cloud.acronis.com>.
 - On the sidebar of Acronis True Image 2018, click **Backup**, click **Add backup**, click the **Backup source** area, and then select **Social network**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, click **Add**, and then choose **Instagram**.
4. Click **Back up Instagram**.
5. Log in to your Instagram account, if prompted.
6. Click **Authorize** to allow Acronis True Image 2018 to access information from your Instagram account (media and profile information). The information will only be used for backup purposes.
7. Configure the backup by setting a schedule for the backup. You can also encrypt the backup and protect it with a password. When done, click **Create**.
8. To start the backup, click **Run now**.

2.9 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.
 - **Nonstop** (available for file-level cloud backup only)
The initial full backup contains all of the data selected for protection. Acronis True Image 2018 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 **Apply**.

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.

2.10 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 set or change the backup encryption option for a pre-existing backup.

To encrypt a backup:

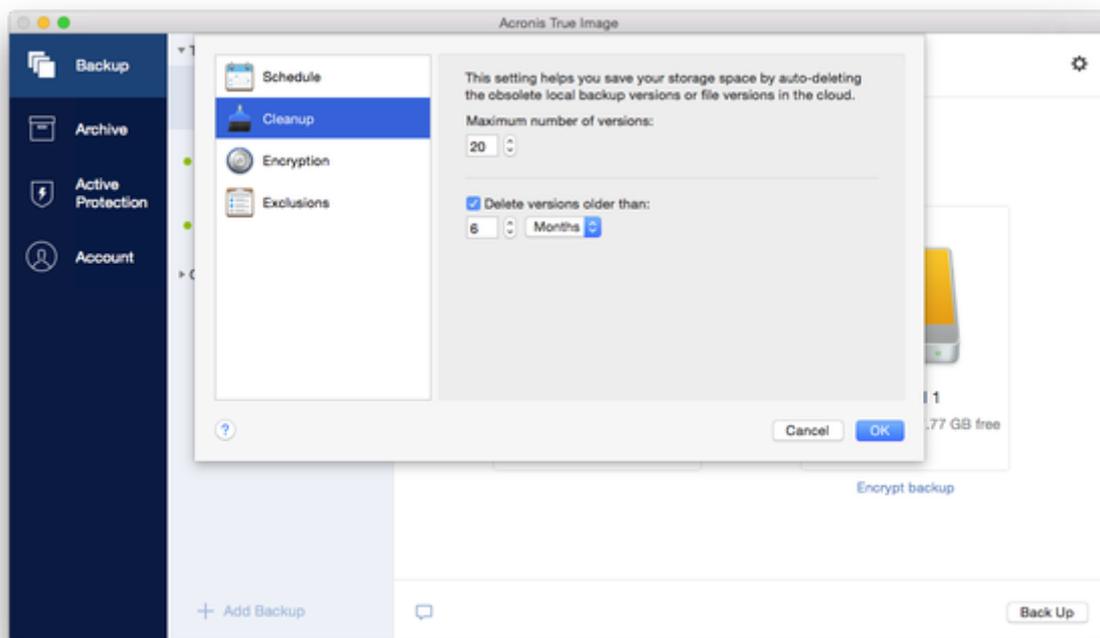
1. When configuring the first backup process, click the **Settings** icon, and then click **Encryption**.
2. Enter the password for the backup into the corresponding field, and then click **OK**.

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.

2.11 Backup retention rules

Every time you run a backup operation, manually or on a schedule, Acronis True Image 2018 creates a new backup version in the backup location. By default, Acronis True Image 2018 stores 20 recent versions. This rule applies to both Acronis Cloud and local or network folders. When you create the twenty-first version, Acronis True Image 2018 automatically deletes the oldest version of the backup. You can change the default value and set a different limit on the number of backup versions.



In addition to the number of versions, you can limit their age. Select the **Delete version 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.

Nonstop backup retention rules

When you back up files and folders to Acronis Cloud, you can select the Nonstop scheduling setting. Refer to Scheduling (p. 25) for details.

Because Acronis True Image 2018 permanently monitors the backed-up data and uploads the changes to Acronis Cloud, the backup could consume the storage space quite fast. To reduce the number of backup versions and optimize the cloud space consumption, Acronis True Image 2018 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.

2.12 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.

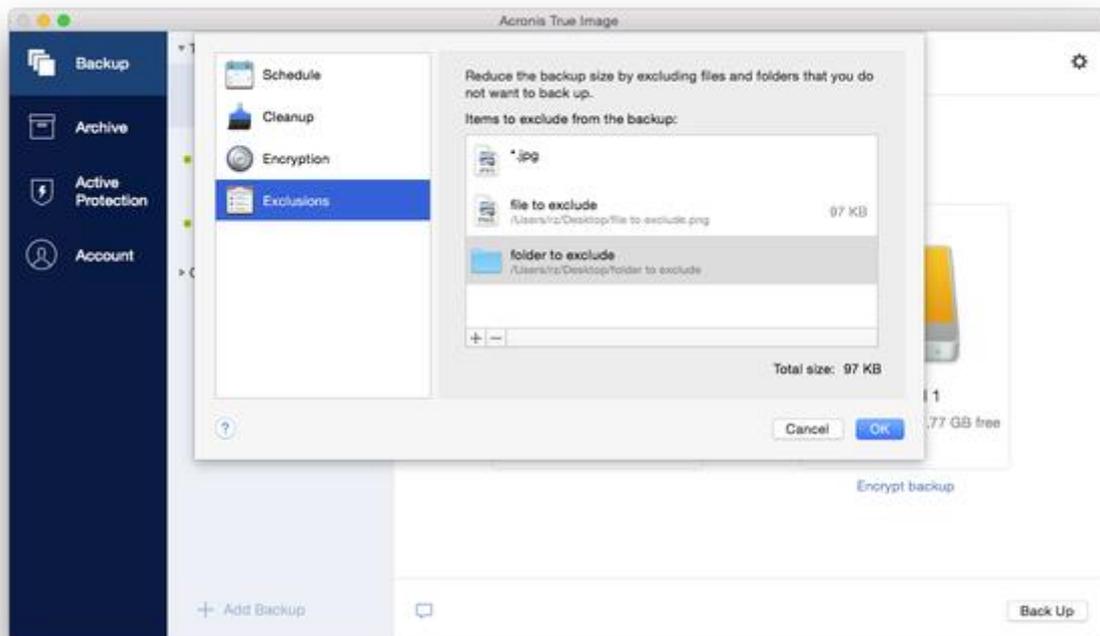
You can exclude files and folders the following ways:

- **Manually, from any backup**
To exclude an item, specify it explicitly or use a mask.
- **Automatically, from a backup to Acronis Cloud**
Acronis True Image 2018 analyzes the backup source and suggests that you exclude your local data that can be downloaded from third-party Cloud storage.

Excluding items manually

To exclude files and folders 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**.

Excluding recoverable data from online backups

Acronis True Image 2018 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

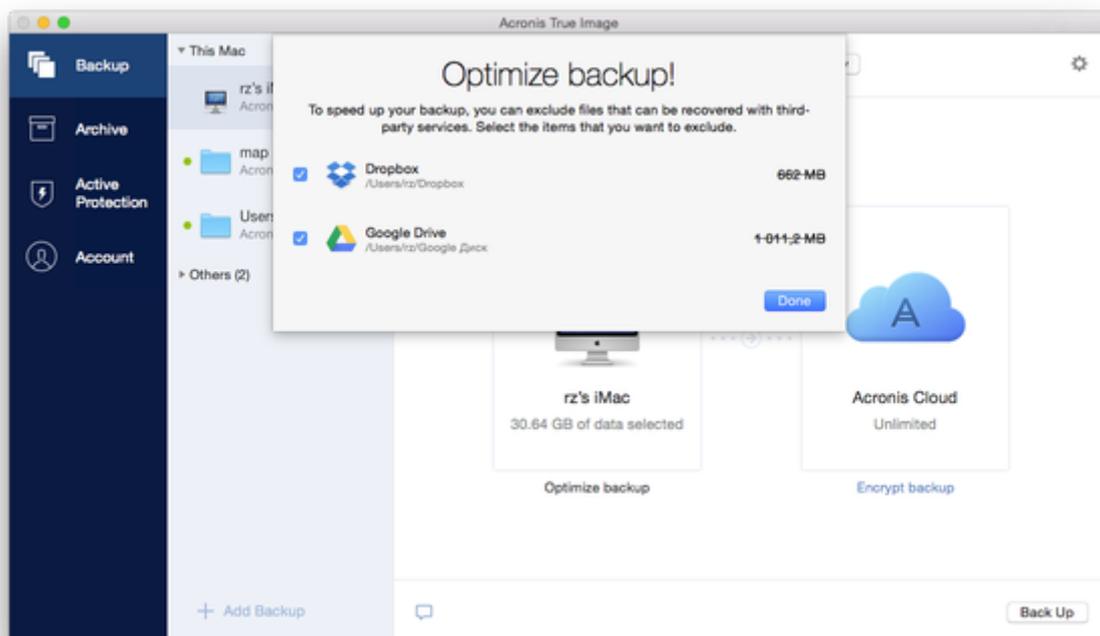
- Google Drive
- BoxSync
- Yandex.Disk
- SugarSync

Acronis True Image 2018 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. Clear the check boxes next to the items that you want to exclude, and then click **Done**.

2.13 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 True Image 2018.
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.

2.14 Network settings for backup

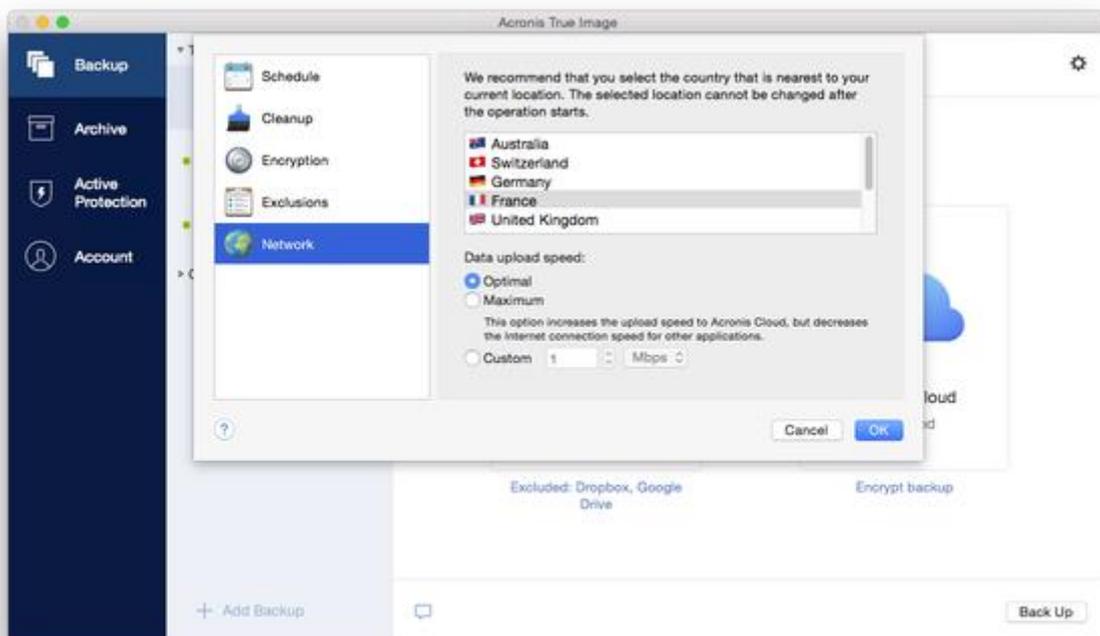
When you create a backup to Acronis Cloud, your data is uploaded to one of the Acronis data centers located in different countries. Initially, the data center is defined as the one closest to your location when you create your Acronis account. Afterwards, your online backups and synced files are stored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



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

Data upload speed

When you back up data to Acronis Cloud, network drives, or FTP, you can change the connection speed used by Acronis True Image 2018. Set the connection speed that will allow you to use Internet and network resources without annoying slowdowns.

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

- **Optimal**
The data transfer rate is not changed by Acronis True Image 2018.
- **Maximum** (available for online backups only)

This option significantly speeds up the upload process, but at the same time the Internet connection speed decreases for other applications. The optimization mechanism splits the data into small portions, and then uploads these portions via multiple network connections. In the target Acronis data center, the split data is assembled back to the initial state, and then stored in the cloud storage.

- **Custom**

You can specify a maximum value for data upload speed.

2.15 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, results of backup validation, etc.

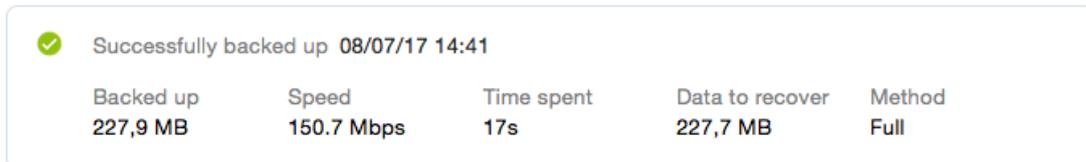
When you create the first version of a backup, the Backup tab displays a graphical representation of the backup content by file types.

The Activity tab

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**.



Backed up	Speed	Time spent	Data to recover	Method
227,9 MB	150.7 Mbps	17s	227,7 MB	Full

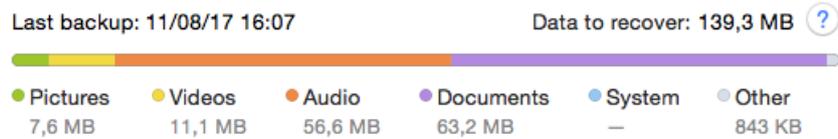
What you can view and analyze:

- 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>.

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

Information on the data size:

- **Data to recover**—size of the original data that you selected to back up.

2.16 Laptop power settings

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. Long-term backups may consume the battery power quite fast, for example when you back up significant amount of data to the cloud.

To save the battery charge:

- In the **Acronis True Image** menu, click **Preferences**, and then select the **Do not back up when working on battery power** check box.

When this setting is turned on and you unplug your laptop power adapter or use UPS for your computer after a blackout, 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 suspended 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.

2.17 Notifications

In-product notifications

You can duplicate Acronis True Image 2018 notifications in OS X Notification Center to view them in usual place and without opening the Acronis True Image 2018 console.

To duplicate in-product notifications in Notification Center:

- In the **Acronis True Image** menu, click **Preferences**, and then select the **Show notifications in Notification Center** check box.

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 True Image** menu, click **Account > 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**.

2.18 What is Acronis Cloud?

Remote storage

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

If you use Acronis True Image 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 True Image 2018.
2. Create Acronis account (p. 34), if you do not have one.
3. In the **File** menu, point to **Acronis Cloud Storage**, and then click **Start Trial** or **Buy Subscription**.

Web application

On the other hand, Acronis Cloud is a web application that allows you to recover and manage the data that you store on Acronis Cloud. To work with the application, you can use any Mac or PC that is connected to the Internet.

To access the application, go to <https://www.acronis.com/my/online-backup/>, log in to your account, and then click **Recover my data now**.

2.18.1 Creating an Acronis account

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

To create an Acronis account:

1. Open Acronis True Image 2018.
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.

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.

2.18.2 Subscription to Acronis Cloud

The Acronis True Image 2018 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 True Image 2018, go to the File menu, point to Acronis Cloud Storage, and then choose if you want to start a trial subscription or buy a full one.

Please note that Acronis Cloud is subject to our Fair Usage Policy. See more details at: <https://kb.acronis.com/atih2018/fairusage>.

Trial version

When you activate the trial version of the product, a 1000 GB storage and 30-day free subscription to Acronis Cloud 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.

Full version

To purchase the full Acronis Cloud Storage subscription:

1. Open Acronis True Image 2018.
2. In the **File** menu, point to **Acronis Cloud Storage**, and then click **Buy Subscription**.
3. Follow the on-screen instructions to proceed with the purchase.

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

2.19 Parallels Desktop support

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 Mac OS X, Linux, Google Chrome OS, and other operating systems. For more details, please visit the Parallels website: <http://www.parallels.com/products/desktop/>.

How does Acronis True Image 2018 handle Parallels Desktop virtual machines?

Acronis True Image 2018 provides complete support of your virtual machines created with Parallels Desktop 9 and later versions. When you back up your Mac, the virtual machines are backed up as well. When you recover your Mac, the virtual machines are reverted to the state they were in when the backup started. After recovery, all your virtual machines remain consistent and bootable.

How does it work?

Every time you run a backup, Acronis True Image 2018 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.

Which virtual machines are backed up?

Acronis True Image 2018 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

How do I recover virtual machines?

To keep bootability of your Parallels Desktop virtual machines, recover entire Mac. Refer to *Recovering your Mac* (p. 39) for details.

In any other case, the virtual machines will not boot after recovery. To restore the bootability, run the `recreate_pd_hdd.sh` script. Since Acronis True Image 2017, the script is shipped with the product and is located in `/Applications/Acronis True Image.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 True Image.app/Contents/MacOS/recreate_pd_hdd.sh"  
"/Users/John/Downloads/My Windows Virtual Machine.pvm"
```

Limitations

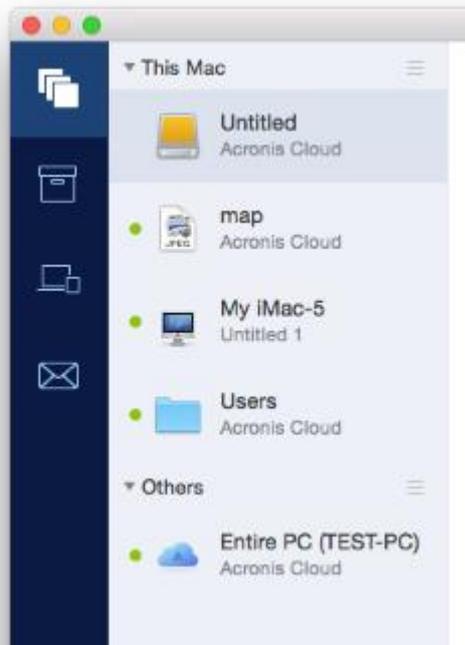
If you have Parallels Desktop virtual machines configured to use the Boot Camp partition, pay attention to the following limitations:

- 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.

2.20 Backup list icons

While working with the backup list, you will see special icons. The icons give you the following information:

- Backup type
- Backup current state



Backup type icons:

Icon	Description
	Entire Mac backup <i>Note: The appearance of this icon depends on the type of your Mac.</i>
	Disk-level backup
	File-level backup of folders or several files.
	File-level backup of a single file.

Backup state indication:

Icon	Description
	The backup successfully completed.
	The backup is queued.
 (blinking)	The backup is in progress.

○	The backup was paused by user.
●	The last backup failed.
●	The backup completed with warnings.

2.21 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. The order is as follows: entire PC backups - disk backups - file backups - nonstop backup.
	Destination type	This command sorts all backups by the destination type. The order is as follows: internal disk drives - external disk drives - NAS devices - network shares - Acronis Cloud.

3 Creating bootable rescue media

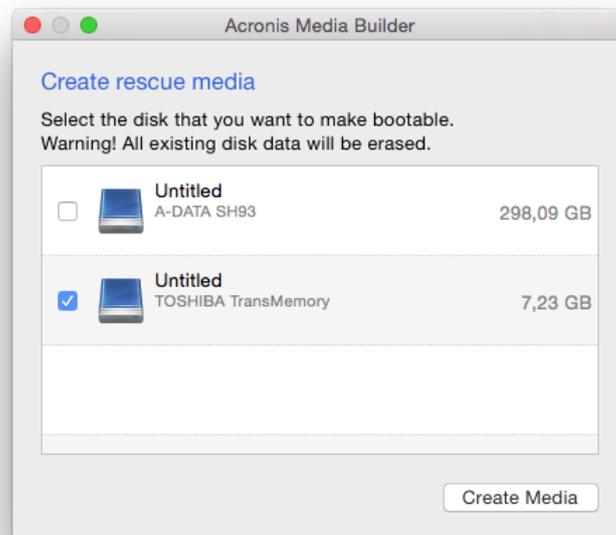
Bootable rescue media is a removable drive containing boot files. When your Mac does not start, you use the drive to boot the Acronis recovery environment and recover your Mac from a previously created backup.

If you do not have a backup yet, please create it. Refer to Backing up to local or network storage (p. 14) and Backing up to Acronis Cloud (p. 15) for details.

 *Using bootable media is the only way to recover your Mac from an Acronis True Image 2018 backup.*

To create Acronis bootable rescue media:

1. Connect a removable drive to your Mac.
The drive must have 4 GB (or more) 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 True Image 2018.
3. In the **File** menu, click **Create Rescue Media**. The Acronis Media Builder window opens.
4. Select the drive that you want to make bootable.



5. Click **Create Media**. If the drive is not empty, Acronis True Image 2018 will ask you to confirm deleting all the data stored on the drive. To confirm, click **Erase**.
6. When the progress is complete, 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.

We recommend that you create a new rescue media every time you upgrade your Mac OS X to a newer version. Otherwise, your rescue media may not work properly.

4 Recovery

In this section

When do I recover my Mac?	39
Recovering your Mac	39
Recovering your files.....	41
Recovering cloud data from any device.....	42
Recovering your Facebook account	44
Recovering your Instagram account	44
Searching backup content.....	45
Network connection transfer rate	45

4.1 When do I recover my Mac?

When your computer does not start up or you notice that your Mac OS X 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 (p. 39) 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 True Image backup. Refer to Recovering your Mac (p. 39) for details.
- If the Disk Utility does not detect any errors, recover your Mac from a Acronis True Image backup. Refer to Recovering your Mac (p. 39) for details.

4.2 Recovering your Mac

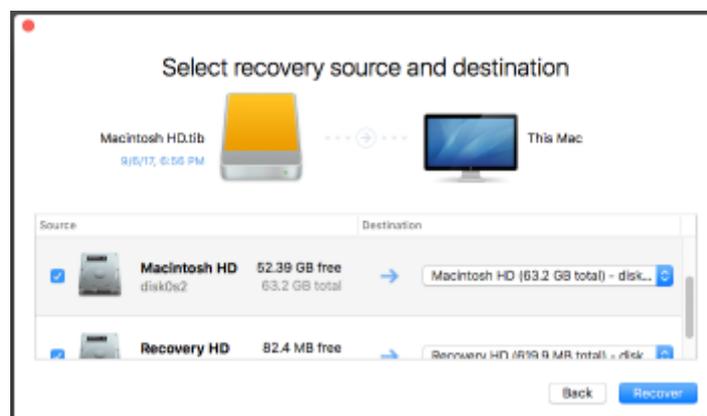
Follow the instructions below to recover your Mac when it cannot start or when it is working incorrectly.

To recover your Mac:

1. Make sure that you have:
 - A previously created Acronis True Image backup. Without the backup recovery is impossible. Refer to Backing up to local or network storage (p. 14) and Backing up to Acronis Cloud (p. 15) for details.
 - Acronis bootable rescue media. If you do not have one and you can start Acronis True Image 2018 on your Mac, please create the media as soon as possible. Refer to Creating bootable rescue media (p. 38) for details.
2. Plug in the bootable media to your Mac.
3. Start or restart your Mac. Press and hold the **Option** key while the Mac is starting. The boot menu will be displayed.
4. Choose Acronis Media as a device to boot from. The **OS X Utilities** list is displayed.



5. Select **Recover from Acronis True Image Backup**, and then click **Continue**.
6. In the window that opens, choose the location of your backup:
 - **Local Storage**
 - **Acronis Cloud**—sign in to your Acronis account.
 - **Network**
 Select your backup, and then click **Open**.
7. 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.
8. Select the check boxes next to the partitions that you want to recover.



9. Select a destination for each partition.

10. To start recovery, click **Recover**, and then confirm that you want to erase all data on the destination partitions.
11. 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 True Image 2018 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 OS X, 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, such as Acronis Cloud, 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 rescue media.
 4. Recover your Mac from the backup to the new hard drive.

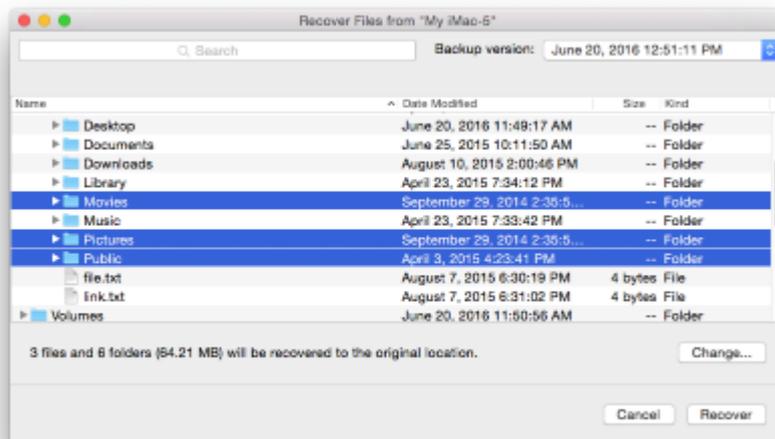
4.3 Recovering your files

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

To recover files and folders:

1. Open Acronis True Image 2018.
2. 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.



3. 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.
4. Select the files or folders that you want to recover.
5. [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.
6. [Optional step, available for cloud backups only] Click **Options**, and then configure the download speed. Refer to Network connection transfer rate (p. 45) for details.
7. 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 True Image 2018 will additionally verify the authenticity of the recovered files.

4.4 Recovering cloud data from any device

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 application.

To open the Acronis Cloud web application, do one of the following:

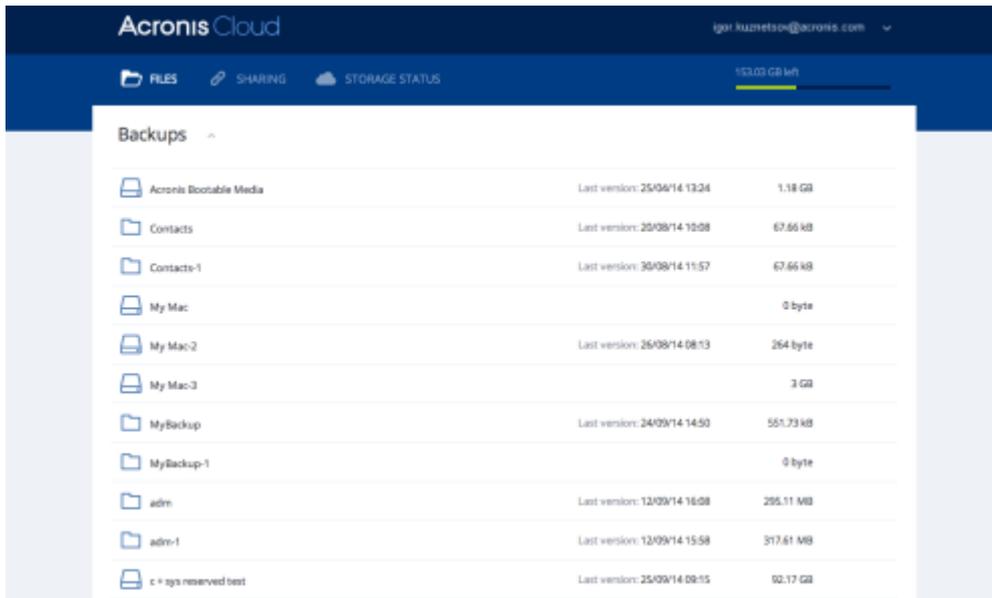
– On your Mac with Acronis True Image 2018 installed:

1. Open Acronis True Image 2018.
2. On the left pane, select the backup that contains files and folders to recover.
3. On the right pane, click **Browse Files**.

– 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.



Recovering the latest versions of files and folders

To recover files and folders:

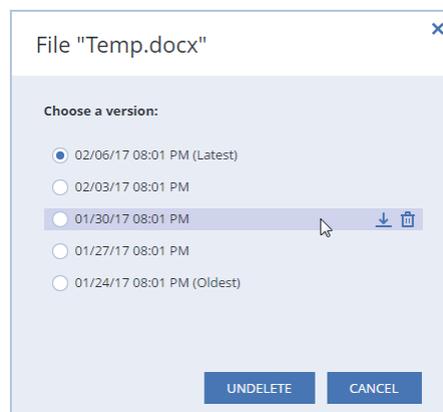
1. On the **Files** tab of the Acronis Cloud web application, browse to the file or folder that you want to recover. You can also use the Search field.
2. To start recovery, click **Download**.
The selected data will be downloaded to the **Downloads** folder.

Recovering the previous file versions

Note that this option is not applicable to folders.

To recover a specific file version:

1. On the **Files** tab of the Acronis Cloud web application, browse to the file that you want to recover. You can also use the Search field.
2. Select the file, click the gear icon to the right of the file, and then click **View versions**.
3. In the window that appears, point to the required version, and then click the **Download** icon.



By default the data will be downloaded to the **Downloads** folder.

4.5 Recovering your Facebook account

Acronis True Image 2018 allows you to protect your entire Facebook account from losing your photos, posts, profile information, and other data and activities. When you have a cloud backup of your account data, you can browse it and recover specific items.

To browse and recover your Facebook data:

1. Open Online Dashboard by doing one of the following:
 - Follow the link: <https://cloud.acronis.com>.
 - On the sidebar of Acronis True Image 2018, click **Account**, and then click **Open Online Dashboard**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, and then find the Facebook backup box.
4. Do one of the following:
 - To recover account data, click the gear icon, click **Recover account**, choose a destination account, select the items that you want to recover, set the privacy settings, and then click **Recover**.
 - To recover specific items, click **Browse data**. 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):

- **View original**—click to view the selected item on Facebook.
- **Show content**—click to view the item details or open it in full size.
- **Recover** (available in Acronis True Image 2017 and later)—click to recover data to your current Facebook account or to a different one. You can also set the privacy settings for the items that you recover.
- **Download**—click to download the selected file.
- View an item's comments, likes, tagged users, and detailed information.

4.6 Recovering your Instagram account

When you have a cloud backup of your Instagram account data, you can browse it and download the backed-up photos and videos.

Note: Instagram does not support recovery of posts or profile information to the Instagram application. You can only download them.

To browse and recover your Instagram data:

1. Open Online Dashboard by doing one of the following:
 - Follow the link: <https://cloud.acronis.com>.
 - On the sidebar of Acronis True Image 2018, click **Account**, and then click **Open Online Dashboard**.
2. Sign in to your Acronis account.
3. On the sidebar, click **Resources**, and then find the Instagram backup box.
4. Click **Browse data**.
5. Do one of the following:

- To view the profile information, click **Profile**.
- To view the backed-up posts, click **My Feed**.

Then you can:

- Browse them the same way you do in your Instagram application.
- Click **Original** to view the selected post in the Instagram application.
- Download specific photos and videos.
- Click **Download all** to download all of the backed-up photos and videos.

4.7 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 (p. 41).
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 True Image 2018 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.

4.8 Network connection transfer rate

When you recover data from Acronis Cloud, network drives, or FTP, you can change the connection speed used by Acronis True Image 2018. Set the connection speed that will allow you to use Internet and network resources without annoying slowdowns.

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

- **Optimal**

The data transfer rate is not changed by Acronis True Image 2018.

- **Maximum** (available for online backups only)

This option significantly speeds up the download process, but at the same time the Internet connection speed decreases for other applications. The optimization mechanism splits the data into small portions, and then downloads these portions via multiple network connections. On your computer, the split data is assembled back to the initial state.

5 Protecting family data

In this section

What is family data protection?	46
Adding a new device	46
Backing up any computer	46
Recovering data with Online Dashboard	47

5.1 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 Acronis 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, Mac OS X, 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.

5.2 Adding a new device

With Online Dashboard, you can add a new device to the device list.

To add a new device to the device list:

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

5.3 Backing up any computer

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

If a device is not yet protected, you can back up it by using the default settings. Acronis True Image 2018 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 True Image 2018 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 Acronis 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 True Image 2018 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 True Image 2018 creates a new full backup and uploads it to Acronis Cloud.

5.4 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 Acronis 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**.

6 Archiving data

In this section

What is data archiving?.....	48
What is excluded from archives?.....	49
Cloud archiving vs. Online backup	49
Archiving your data	50
Accessing your archived files	52

6.1 What is data archiving?

Data archiving is a tool that allows you to move your big or rarely used files to Acronis Cloud, NAS, an external hard drive, or a USB flash drive. Every time you run this tool, it analyzes the data in the selected folder and suggests uploading the found files to Acronis Cloud or moving them to local storage. 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: Acronis Cloud or local storage, such as an internal hard drive, external hard drive, NAS, or a USB flash drive. 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 True Image 2018, the Acronis True Image mobile application, and the Acronis Cloud web application from any device running Windows, Mac OS X, 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 True Image 2018 keeps all the modifications in different file versions. You can choose a previous file version and download it to your device.

6.2 What is excluded from archives?

To reduce archive size and eliminate a possibility to corrupt your system, by default Acronis True Image 2018 excludes the following data from archives:

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

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

6.3 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.

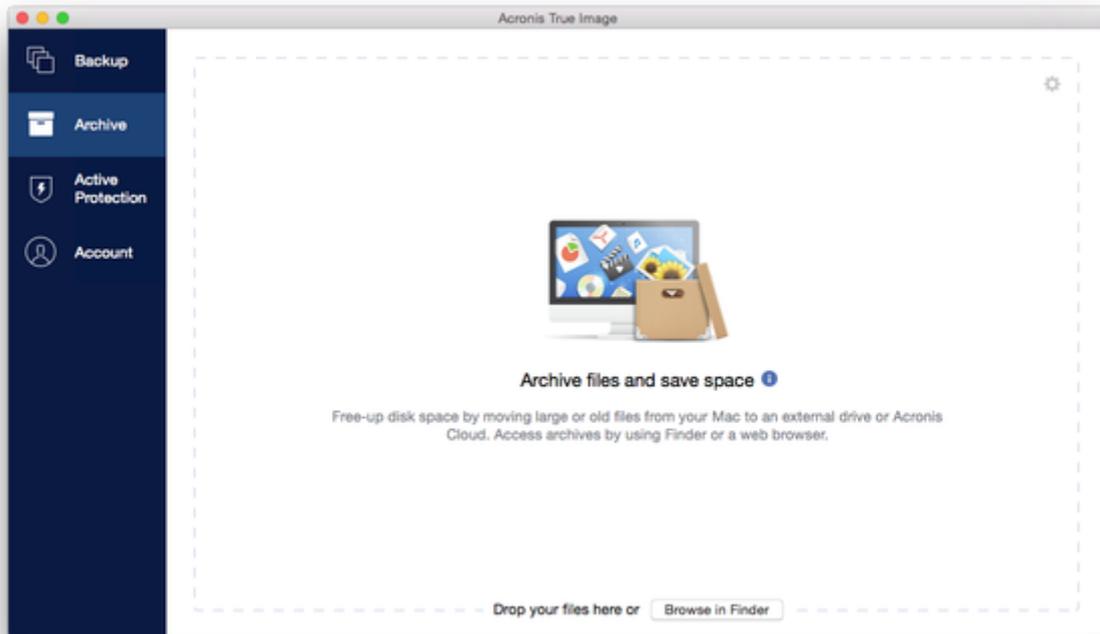
	Online backup	Cloud archiving
Feature purpose	Data protection from operating system corruption, hardware failures, and loss of separate files.	Cleanup of local storage device and moving data to Acronis Cloud.
Data protection	<ul style="list-style-type: none"> ▪ Overall protection of all data on a computer, 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 change frequency	The data to back up is changed frequently. Usually a backup has many versions updated from time to time.	The data to archive is changed rarely. The files have few versions.

6.4 Archiving your data

Data archiving helps you free up your storage space by moving your old or rarely used files to Acronis Cloud or local storage. Refer to What is data archiving (p. 48) for details.

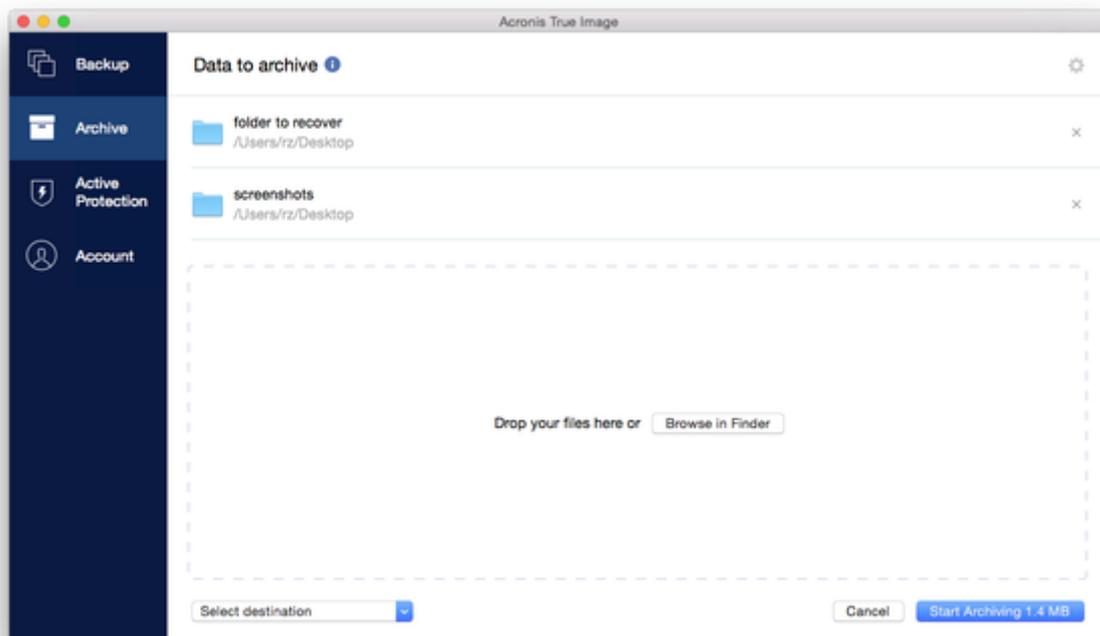
To archive your data:

1. Start Acronis True Image 2018, 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 Acronis Cloud or a custom local 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 (p. 52) for details.
 - Select a preferred data center and configure the upload speed at **Settings** → **Advanced**. Refer to Selecting Acronis Cloud data center (p. 30) 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.

6.4.1 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 True Image 2018. 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:

- **Optimal**
The data transfer rate is not changed by Acronis True Image 2018.
- **Maximum**
This option significantly speeds up the upload process, but at the same time the Internet connection speed decreases for other applications. The optimization mechanism splits the data into small portions, and then uploads these portions via multiple network connections. In the target Acronis data center, the split data is assembled back to the initial state, and then stored in the cloud storage.
- **Custom**
You can specify a maximum value for data upload speed.

6.4.2 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.

6.5 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)
Open the Acronis Cloud web application in one of the following ways:
 - Open Acronis True Image 2018, click **Archive**, and then click **Open in web browser**.
 - Go to <https://www.acronis.com/my/online-backup/>, log in to your account, and then click **Recover my data now**.

7 Tools

In this section

Acronis Active Protection.....53

7.1 Acronis Active Protection

What is ransomware?

Ransomware is malicious software that blocks access to some of your files or entire system and demands a ransom for unblocking. The software shows you a window informing you that your files are locked and that you have to pay urgently, otherwise you will not be able to access the files anymore. The message may also be disguised as an official statement from authorities, for example, the police. The purpose of the message is to frighten a user and make them pay without asking for help from an IT specialist or the authorities. Moreover, there is no guarantee that you will regain control over your data after paying the ransom.

Your computer can be attacked by ransomware when you visit unsafe websites, open email messages from unknown people, or when you click suspicious links in social networks or instant messages.

Ransomware can block your access to:

- **Entire computer**
You cannot use Mac OS X or do anything on your computer. As a rule, ransomware does not encrypt your data in this case.
- **Specific files**
Usually, this is your personal data, such as documents, photographs, and videos. Ransomware encrypts the files and demands money for the encryption key, which is the only way to decrypt your files.
- **Applications**
Ransomware blocks some of your programs so that you cannot run them. It most often attacks your web browser.

How Acronis True Image 2018 protects your data from ransomware

To protect your computer from ransomware, Acronis True Image 2018 uses the Acronis Active Protection technology. Based on a heuristic approach, this technology monitors processes running on your computer by using the real-time mode. When it detects a third-party process that tries to encrypt your files or inject malicious code into a healthy process, it informs you about it and asks if you want to allow the process to modify your files or block the process. Refer to Protecting your data from ransomware (p. 54) for details.

A heuristic approach is widely used in modern antivirus software as an effective way to protect data from malware. As opposed to the signature-based approach which can detect only one sample, heuristics detects malware families that include samples with similar behavior. One more advantage of this approach is an ability to detect new kinds of malware that do not have a signature yet.

Acronis Active Protection uses behavioral heuristics and analyzes chains of actions done by a program, which is then compared with the chain of events in a database of malicious behavior patterns. Since this method is not precise, it admits so-called false positives, when a trusted program

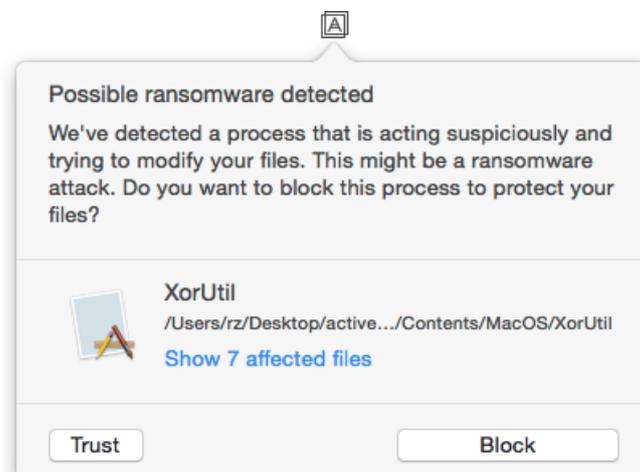
is detected as malware. To eliminate such situations, Acronis Active Protection asks you if you trust the detected process. When the same process is detected for the second time, you can add it to the permission list and set the default action for this process by marking it as trusted or blocked. If you do not, you will be able to blacklist this process. In this case, this process will be blocked every time it tries to modify your files.

To collect as many as possible different patterns, Acronis Active Protection uses Machine Learning. This technology is based on mathematical processing of big data received with telemetry. It is a self-learning approach, because the more data is processed, the more precisely a process may be detected as ransomware or not.

In addition to your files, Acronis Active Protection protects the Acronis True Image application files, your backups, and archives.

7.1.1 Protecting your data from ransomware

When the Acronis Active Protection service is on, it monitors the processes running on your computer by using the real-time mode. 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 modify your files or block the process.



Before you make your decision, you can view the list of files that the process is going to modify.

To allow the process to modify the files, click **Trust**. If you are not sure if the process is safe and legal, we recommend that you click **Block**. In any case, next time the process is run Acronis True Image 2018 will ask you again. To give the process permanent permission or to block it every time it tries to modify your files, select the **Remember my choice for this process** check box, and then click **Block** or **Trust**. The process will be added to the permission list. You can manage the list in Settings.

After blocking the process, we recommend that you check if your files have been encrypted or corrupted in any way. If this is the case, click **Recover modified files**. Acronis True Image 2018 will search the latest file versions and recover the files from one of the following:

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

To make this action the default, select the **Always recover files after blocking a process** check box.

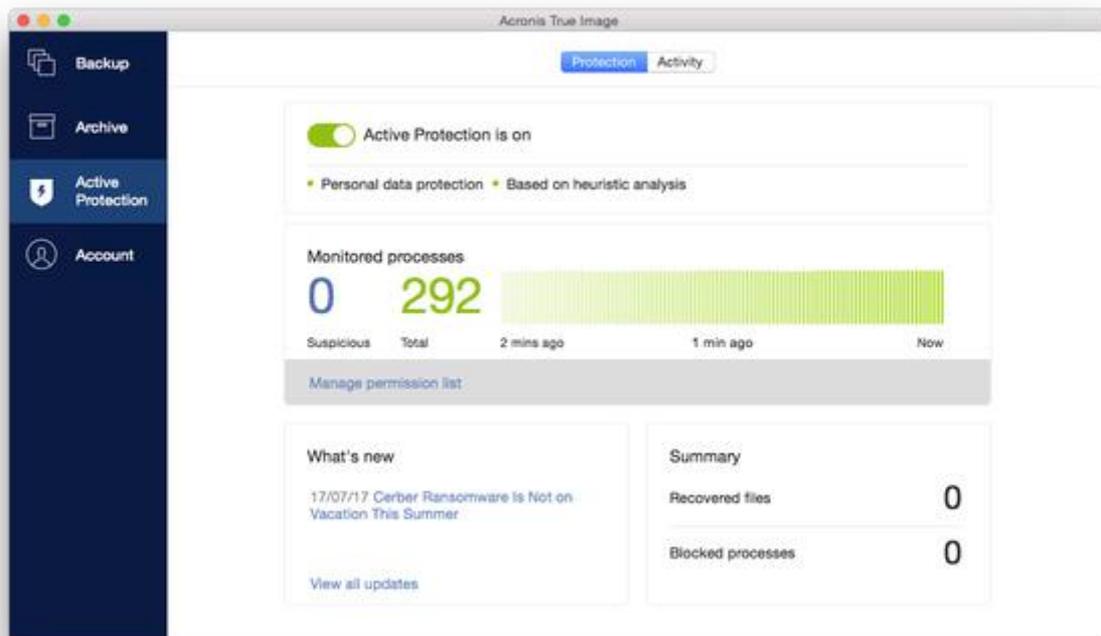
7.1.2 Acronis Active Protection settings

When the Acronis Active Protection service is on, it monitors the processes running on your computer by using the real-time mode. 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 modify your files or block the process.

Acronis Active Protection dashboard

The dashboard represents a number of statistic data on the protection process and allows you to configure the main Acronis Active Protection settings, such as permission list and exclusions.

To open the dashboard, start Acronis True Image 2018, and then click **Active Protection** on the sidebar.



The dashboard allows you to:

- Turn the Acronis Active Protection service on and off
- Manage the permission list
This list allows you to trust or block applications.
- Manage exclusions
Use the exclusion list to specify files and folders that you do not want to protect from ransomware.
- Monitor in real-time mode:
 - The current number of the processes being analyzed
 - The current number of protected files
- Read the data protection-related articles

Status icon on the macOS menu bar

The Acronis Active Protection utility has its own status icon on the menu bar.



Clicking the icon opens the following menu items:

- **Open Acronis True Image**—click to open the Acronis Active Protection dashboard.
- **Turn Off Acronis Active Protection (Turn On Acronis Active Protection)**—click to turn the ransomware protection off or on.
- **Manage Processes**—click to open the list of applications added to the permission list. Each application is marked as blocked or trusted. You can add and remove applications from the list and change their status.
- **Help**—click to open Help for Acronis Active Protection.

Copyright Statement

Copyright © Acronis International GmbH, 2002-2018. All rights reserved.

"Acronis", "Acronis Compute with Confidence", "Acronis Recovery Manager", "Acronis Secure Zone", "Acronis True Image", "Acronis Try&Decide", and the Acronis logo are trademarks of Acronis International GmbH.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <http://kb.acronis.com/content/7696>

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.