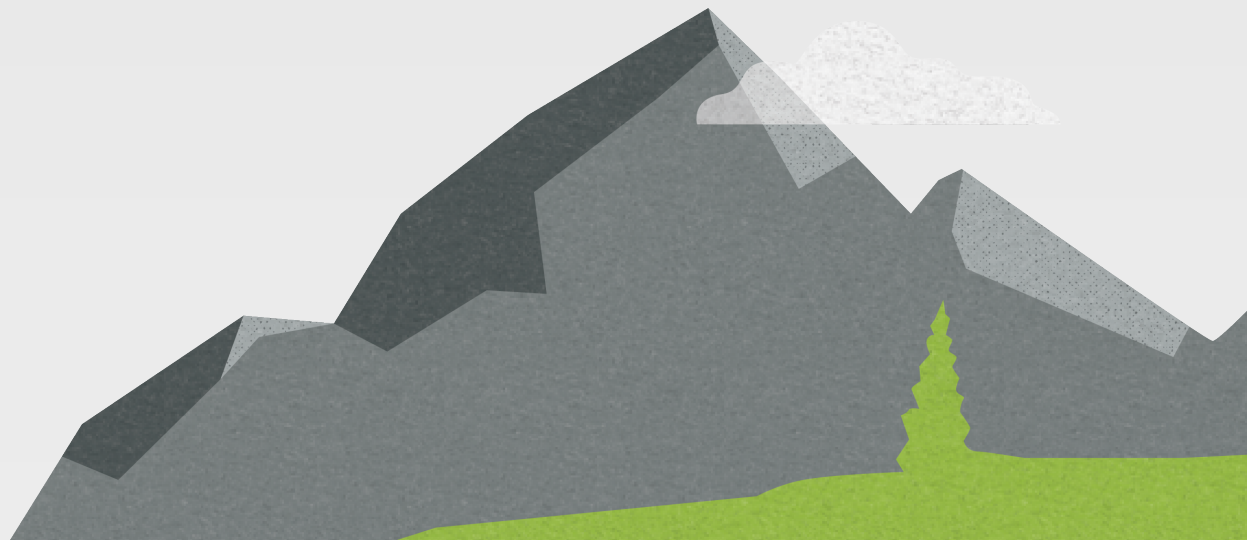


## *User Guide*



## Notices

Carbonite Endpoint User Guide, version 10.12, June 2023

© 2023 Open Text. All rights reserved.

One or more patents may cover this product. For more information, please visit

<https://www.opentext.com/patents>.

If you need technical assistance, you can contact Customer Support. All basic configurations outlined in the online documentation will be supported through Customer Support. Assistance and support for advanced configurations may be referred to a Pre-Sales Systems Engineer or to Professional Services.

This documentation is subject to the following: (1) Change without notice; (2) Furnished pursuant to a license agreement; (3) Proprietary to the respective owner; (4) Not to be copied or reproduced unless authorized pursuant to the license agreement; (5) Provided without any expressed or implied warranties, (6) Does not entitle Licensee, End User or any other party to the source code or source code documentation of anything within the documentation or otherwise provided that is proprietary to OpenText; and (7) All Open Source and Third-Party Components (“OSTPC”) are provided “AS IS” pursuant to that OSTPC’s license agreement and disclaimers of warranties and liability.

Open Text and/or its affiliates and subsidiaries in the United States and/or other countries own/hold rights to certain trademarks, registered trademarks, and logos. Microsoft and Azure are registered trademarks of the Microsoft group of companies. macOS is a registered trademark of Apple Inc. Okta is a registered trademark of Okta, Inc.. All other trademarks are the property of their respective companies. For a complete list of trademarks registered to other companies, please visit that company’s website.

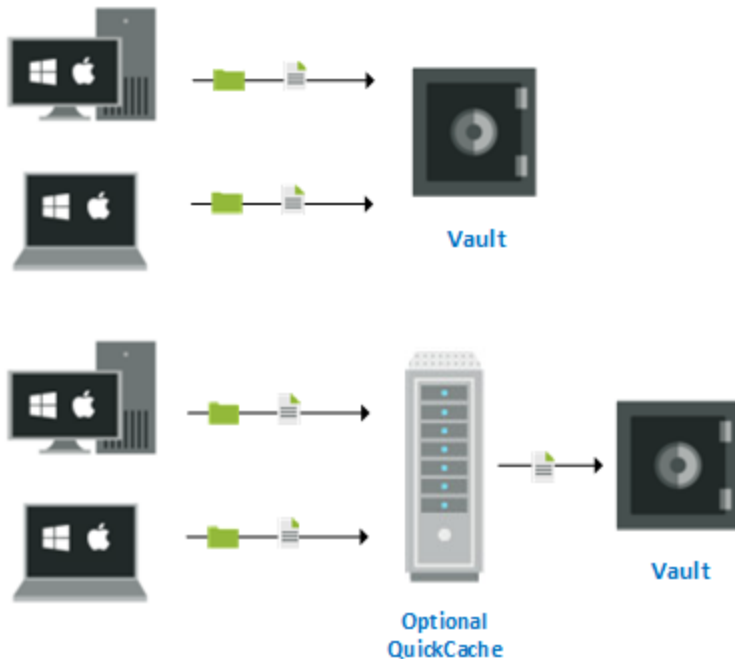
# Contents

---

<b>Overview</b>	<b>4</b>
<b>Get started</b>	<b>5</b>
<b>Requirements</b>	<b>6</b>
<b>Install Carbonite Endpoint</b>	<b>8</b>
<b>Console</b>	<b>11</b>
<b>Protect files</b>	<b>13</b>
Configure self-managed protection	14
Configure hybrid protection	18
Configure the protection settings	22
<b>Restore files</b>	<b>24</b>
Restore using the Carbonite Endpoint console	25
Restore files using the web retrieval site	28
Log in to the web retrieval site with two-factor authentication	29
Log in to the web retrieval site with an emailed authentication code:	29
Log in to the web retrieval with a code from a mobile authenticator:	30
Set up or remove a mobile authenticator	30
Set up a mobile authenticator:	31
Remove a mobile authenticator:	31
<b>Delete files on the vault</b>	<b>32</b>
<b>Resolve file issues</b>	<b>34</b>

# Overview

Carbonite Endpoint provides backup protection for desktop and laptop data. Desktops and laptops are known as devices or endpoints. All endpoints are backed up to a single location known as the vault. After the initial backup, subsequent backups are smaller and faster because only changes are backed up. An optional QuickCache can be used for faster backups in local environments. Backed up data can be restored from the vault to any device, any time, anywhere. The backup files are immutable and therefore forensically defensible.



To configure protection, an administrator or user selects the files to be backed up and how often the files are checked for changes (default every 15 minutes). Once protection is configured, the files are backed up and protected as long as the computer is running. Protection occurs locally if the computer is not connected to the local network or Internet. The changes are sent to the vault (or optional QuickCache) when the computer is back online. You do not need to take any additional action unless you want to change the protection configuration or restore files. If you want to restore files, they are downloaded from the vault to the original location or a new location. In the event your computer crashes or is stolen, you can restore all of your protected files to your replacement computer.

This document is for users running the Carbonite Endpoint console on their desktop or laptop. It includes information for protecting your data, restoring your data, and erasing your data on the vault.

If your administrator pushed the application to your device, all or part of the console may be disabled. If all of the console has been disabled, you do not need this document because your administrator will be fully controlling the application. If part of the console has been disabled, only parts of this document will be applicable to you, depending on what you have access to.

# Get started

Use the following guidelines to help you get started with Carbonite Endpoint.

1. *Requirements* on page 6—Review this information to make sure your Windows or macOS device meets the minimum requirements.
2. *Install Carbonite Endpoint* on page 8—If your administrator did not push Carbonite Endpoint to your device, you will need to install it manually.
3. *Console* on page 11—Review this section to familiarize yourself with the Carbonite Endpoint interface.
4. *Protect files* on page 13—Use this section when you are ready to select the files you want to protect.

Once protection is configured, your files are backed up and protected, as long as your computer is running. Protection occurs locally if you are not connected to the local network or Internet. The changes are sent to the vault (or optional QuickCache) when you are back online. You do not need to take any additional action unless you want to change the protection configuration or restore files. If you want to restore files, see *Restore files* on page 24, or if you want to delete files on the vault see *Delete files on the vault* on page 32.

# Requirements

Your device must meet the following requirements in order to use Carbonite Endpoint.

- **Windows operating system**—The following Windows operating systems are supported.
  - Windows 11
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7



Arm-based processors are only supported with Windows 11.

Windows Starter Editions are not supported.

---

- **macOS operating system**—The following macOS operating systems are supported.
  - macOS 13 Ventura
  - macOS 12 Monterey
  - macOS 11 Big Sur
  - macOS 10.15 Catalina
  - macOS 10.14 Mojave
  - macOS 10.13 High Sierra
  - macOS 10.12 Sierra



Starting with macOS 10.14 Mojave, the operating system includes a security feature called Full Disk Access (FDA) which blocks applications from accessing specific locations. This may prevent Carbonite Endpoint from backing up and restoring files, such as Apple Mail, Photos, Calendar, and so on. In order to back up and restore these files, you must enable Full Disk Access for Carbonite Endpoint.

## **Enable Full Disk Access on a macOS 12, 11, 10.15 or 10.14 device**

1. Under the Apple icon, click **System Preferences, Security & Privacy**, and on the **Privacy** tab, select **Full Disk Access**.
2. If the padlock icon is locked, click the icon and enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
3. Click **Add an application** (the plus icon), click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.

## **Enable Full Disk Access on a macOS 13 device**

1. Under the Apple icon, click **System Settings, Privacy & Security**, and select **Full Disk Access**.

2. Click the plus icon.
  3. In the Privacy & Security box, enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
  4. Click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
- 

- **File systems**—Case-sensitive file systems are not supported. The file system must be case-insensitive.
- **Operating system language**—Your computer can be running any language and locale. The console will be in English. However, if your administrator offers language support, your console may be localized in one of the following languages.
  - French - France
  - German - Germany
  - Italian - Italy
  - Japanese
  - Korean
  - Polish
  - Portuguese - Brazil
  - Simplified Chinese
  - Spanish - Spain
  - Turkish
- **System memory**—The minimum system memory is 1 GB.
- **Free disk space**—You must have at least 1 GB of free space on your computer.
- **Drives**—Carbonite Endpoint supports local drives only. This includes SAN drives, which appear as local drives. This does not include NAS, which appear as volumes on a file server. Additionally, it does not include cloud-only drives. Features such as OneDrive On-Demand or iCloud are not supported because the files are only stored in the cloud, even though they appear visible locally.

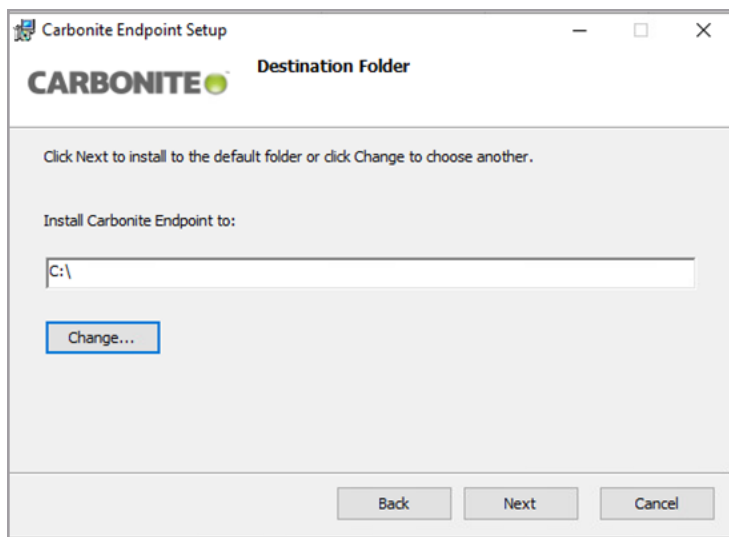
On macOS, only the system drive can be protected.

- **Browser**—You need to have a recent version of a web browser installed.
- **Microsoft .NET Framework**—For Windows computers, Microsoft .NET Framework version 4.6.2 or later must be installed. If you do not have it installed, the Carbonite Endpoint installation can install it for you.

# Install Carbonite Endpoint

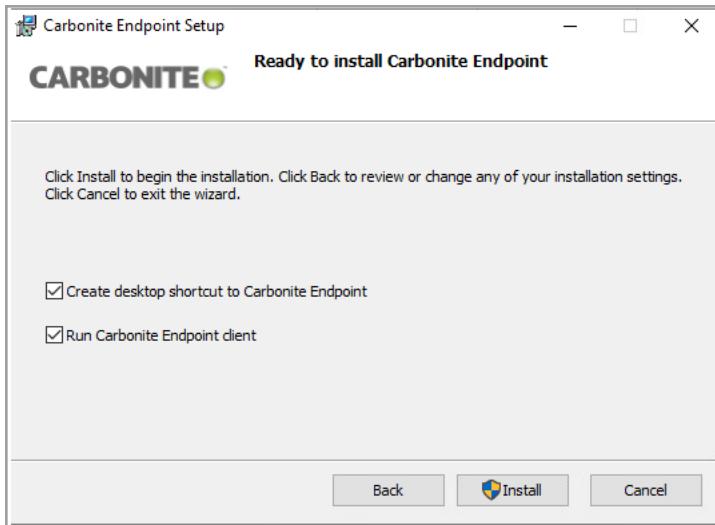
Your administrator may have installed Carbonite Endpoint for you. If not, you must manually install it yourself using the following instructions. These instructions to install Carbonite Endpoint follow the Windows interactive installation wizard. At a high-level, the same process is used on macOS devices, except for a few differences outlined below and a different style interface, such as **Next** buttons that are labeled as **Continue** on macOS devices.

1. Launch the installation file.
2. At the **Welcome** page, click **Next** to continue.
3. Review the **Terms of Service**. You must accept the terms in order to continue with the installation program. Click **Next** to continue.
4. On Windows, modify the installation location, if desired. This option is not available on macOS devices. Carbonite Endpoint will be installed on Macintosh HD.
5. Click **Next** to continue.
6. On Windows, select an internal, local disk that will be used for the local data cache. The drive you select should have at least 1 GB free space. This option is not available for macOS devices. The local data cache will be installed on Macintosh HD.

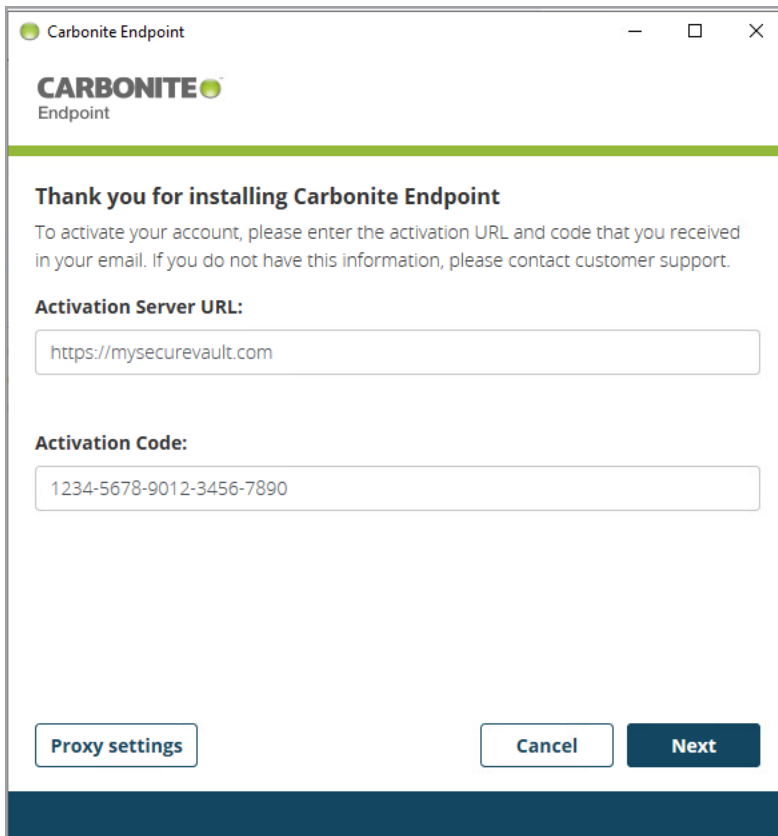


7. Click **Next** to continue.
8. Optionally, deselect the options for the desktop shortcut and running the client after the installation. These options are not shown on macOS devices and will automatically be enabled.





9. When you are ready to begin the installation, click **Install**.
10. When the installation is completed, click **Finish**.
11. In the **Thank you** window that opens after the installation is complete, enter your activation information.



- **Activation Server URL**—This is the URL where files will be backed up. In most cases, you can obtain this URL from an email from your administrator.

- **Activation Code**—This is the activation code for the device. In most cases, you can obtain this activation code from an email from your administrator.
12. If you need to specify a proxy server for Internet access, click **Proxy settings** and complete the proxy information. You can complete the proxy setup after the installation is complete. See *Configure the protection settings* on page 22 for details.
  13. Click **Next** to continue.
  14. If you are reactivating a previously used device, you are prompted to enter a **Passphrase**. Enter it and then click **Next** to continue. You will not see this page if you are not reactivating.
  15. Once the activation is complete and the account is activated, click **Close**.

# Console

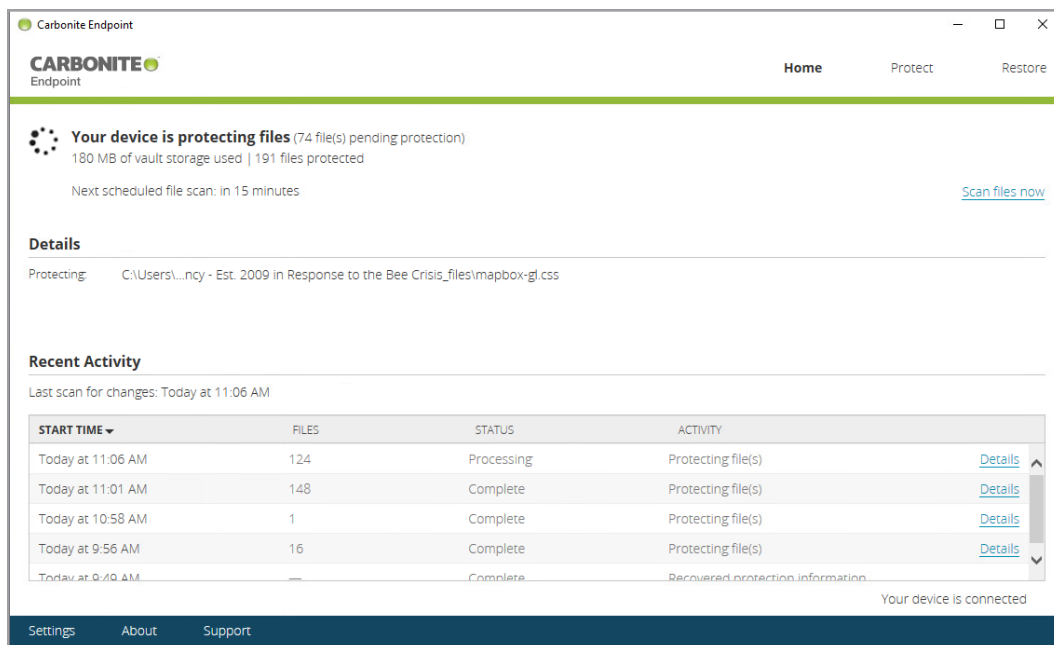
You can protect and restore your files using the Carbonite Endpoint console. Once you have configured your protection, you do not need to have the console running in order for your selected files to be backed up. The files are backed up and protected as long as your computer is running.

You can access the console from the desktop icon if there is one or from **Start** on Windows and from **Launchpad** on macOS.

Three tabs, **Home**, **Protect**, and **Restore** appear at the top right of the console by default. These tabs allow you to access different areas of the application. Your view may vary depending on the access your administrator has granted. A **Settings** link at the bottom left of the console provides access to protection settings and links to console information and help. A status message at the bottom right of the console indicates whether your device is connected to the vault.

Most of your interaction will be with the three navigation tabs.

- **Home**—This is the main tab that displays protection summary and activity details for your protection and restores.



- **Status**—The top section displays the current device status, including whether your device is protected or unprotected and whether your device is in the process of backing up or restoring files. This section also indicates when your next scheduled scan will occur.

If you want to start a manual backup scan immediately, click **Scan files now**. Selecting this option resets the time of your next scheduled scan.

An **Alerts** box displays if you have any issues with your protection. The alert also contains a link to additional information, if it is available. You can click the link to view the alert details. See *Resolve file issues* on page 34 for details.

- **Details**—This section displays information about whether a backup or restore is actively occurring and also includes processing information. If Carbonite Endpoint is not actively scanning or processing files, this section is empty.
- **Recent Activity**—This section displays individual protection scans or restore processes including the time, the number of files backed up or restored, the process status, and the type of activity. Click **Details** to view detailed information on an individual process. Details for other processing activity, for example after a device reset, may not be available.
- **Protect**—This tab is where you configure the files you want to back up. See *Protect files* on page 13 for details.



In addition to configuring the files you want to protect, you can configure the protection process. Click **Settings** in the footer at the bottom of the console. See *Configure the protection settings* on page 22 for more details.

---

- **Restore**—This tab is where you can restore files that have been protected. See *Restore using the Carbonite Endpoint console* on page 25 for details.



Depending on your device configuration, especially if you are running anti-virus or firewall software, you may see the console indicate it is not responding. This is generally a transient issue that will resolve itself. If you find the console frequently not responding, you may want to contact your administrator to see about approving Carbonite Endpoint as a safe application within your anti-virus or firewall.

---

# Protect files

There are three types of protection configurations. Your administrator determines the type you are using.

- **Administrator managed**—Your administrator is controlling which files are and are not protected on your device. If you are configured for this type of protection, the **Protect** tab is not available, and only the **Home** and **Restore** tabs are displayed. The related protection topics are not relevant to this configuration.
- **Self managed**—You control which files are and are not protected on your device. If you are configured for this type of protection, you will see the **Home**, **Protect**, and **Restore** tabs. The **Protect** tab is where you will configure your protection. See *Configure self-managed protection* on page 14 for details.
- **Hybrid**—Your administrator configures default files to protect or not protect on your device, and you have the option to include or exclude additional files if desired. You should initially see an alert on the **Home** page, informing you that you can add additional files if you want to. Once the alert is dismissed, you will not see it again. If you are configured for this type of protection, you will also see the **Protect** and **Restore** tabs. The **Protect** tab is where you can include or exclude additional files. See *Configure hybrid protection* on page 18 for details.

Regardless of your protection configuration, there are default protection settings configured by your administrator. You may or may not be able to override the defaults, depending on the access your administrator has granted. If you are able and so desire, you can modify these settings. See *Configure the protection settings* on page 22 for details.

# Configure self-managed protection

Go to the **Protect** tab. If this tab is not visible, your administrator is controlling protection and this section is not applicable to you.

A self-managed protection configuration is indicated by a table under the **Protect** tab that has check boxes on the left side of each table row. Use this section to configure your self-managed protection. If the table does not have check boxes on the left side of each table row, you have a hybrid protection configuration. See *Configure hybrid protection* on page 18 for details.

The **Protect** tab is divided into two sections.

- **What would you like to protect**—This section contains backup rules that define the files to include in your backup.
- **What would you like to exclude**—This section contains exclusion rules that define the files to exclude from the backup.

The include and exclude sections are defined by a file type and a location. The file type can be pre-defined (all files, documents, email files, music and audio files, photos and images, or videos), or it can be a custom file type that you create. The location can be one specific location or multiple locations.



If you do not see the table of available items in either the protection or exclusions sections, click **See file types**.

What would you like to protect?		
FILE TYPE	LOCATION	
<input type="checkbox"/> All Files	My Documents	<a href="#">Edit</a>
<input type="checkbox"/> Documents	Internal drives	<a href="#">Edit</a>
<input type="checkbox"/> Email Files	Internal drives	<a href="#">Edit</a>
<input type="checkbox"/> Music & Audio	Internal drives	<a href="#">Edit</a>
<input type="checkbox"/> Photos & Images	Internal drives	<a href="#">Edit</a>
<input type="checkbox"/> Videos	Internal drives	<a href="#">Edit</a>
<a href="#">+ Add a file type and location...</a>		

1. Select any of the pre-defined file types and default locations for backup or exclusion by clicking the check box to the left of the item. For a complete list of the file extensions classified within a file type, hover over the file type name or click **Edit** to see the details of the backup or exclusion rule.
  - **All Files, My Documents**—On Windows devices, this option backs up or excludes all files stored in your My Documents folder.
  - **All Files, Documents**—On macOS devices, this option backs up or excludes all files stored in your Documents folder.
  - **Documents, internal drives**—This option backs up or excludes all documents stored on all internal drives on your device.

- **Email Files, internal drives**—This option backs up or excludes all email related files stored on all internal drives on your device.
  - **Music & Audio, internal drives**—This option backs up or excludes all music and audio files stored on all internal drives on your device.
  - **Photos & Images, internal drives**—This option backs up or excludes all photo and image files stored on all internal drives on your device.
  - **Videos, internal drives**—This option backs up or excludes all videos stored on all internal drives on your device.
2. If you want to modify the location of any of the pre-defined file types, use the following steps.
    - a. Click **Edit** to view the rule details.
    - b. Click **Add a specific location**, select a volume or folder, and click **OK**. The location is included or excluded recursively, meaning the rule is automatically applied to the subfolders of the specified path (unless another rule exists for a subfolder).

- c. Repeat the previous step to add multiple locations. Review the caveats below to understand how multiple rules interact with one another.
  - d. If you need to remove a custom location, click **Remove**. Remove all custom locations to go back to the default location.
  - e. Click **Save** to save the modified rule.
3. If you want to create your own file types to back up or exclude, use the following steps.
    - a. Click **Add a file type and location**. If the link is not visible, click **See file types** to expand the table.
    - b. Specify the details for the rule.

- **File type**—Specify a unique and descriptive name for the types of files you want to back up or exclude.

- **File extension details**—Specify the file extensions you want to back up or exclude. If you want to specify more than one extension, separate them with a space. Do not use periods, commas, asterisks, or any other characters specified in the console as invalid.
- **File type location**—Specify the location to look for these types of files. The location is included or excluded recursively, meaning the rule is automatically applied to the subfolders of the specified path (unless another rule exists for a subfolder).
  - a. Click **Add a specific location**, select a volume or folder, and click **OK**.
  - b. Repeat the previous step to add multiple locations. Review the caveats below to understand how multiple rules interact with one another.
  - c. If you want to remove a location, click **Remove**.
- c. Click **Save** to save the custom rule.



If you later want to go back to the default location for a pre-defined file type, go back to **Edit** and **Remove** all locations.

If you later want to delete a custom rule, go back to **Edit** and click **Delete set**.

Keep in mind the following when defining and selecting your rules.

- A rule for a file type will take precedence over a rule for **All Files**.
- In the case of multiple rules, files use the rule that is closest in the folder structure to them. In the following example, all files and folders under My Documents (which is C:\Users\UserName) will be backed up (the first rule). However, video files will be excluded from C:\Users\UserName and its subfolders (the third rule), except the videos located in C:\Users\UserName\Folder1\Folder2 and its subfolders will be included (the second rule).

What would you like to protect?

FILE TYPE	LOCATION	
<input checked="" type="checkbox"/> All Files	My Documents	<a href="#">Edit</a>
<input checked="" type="checkbox"/> Videos	custom	<a href="#">Edit</a>

[See file types](#)

Videos includes the following extensions:

.3g2, .dif, .m4v, .mpeg, .qts, .swf, .3gp2, .dv, .m75, .mpg, .rm, .wm, .3gpp, .flc, .mlv, .mps, .rmvb, .wmd, .amc, .fl, .mov, .mswmm, .rts, .wmv, .asf, .lrf, .mp2v, .mpv2, .rtsp, .wmz, .asx, .m1v, .mp4, .nsv, .rv, ...

Which will be protected in the following location:

C:\Users\UserName\Folder1\Folder2

Click Edit for full details.

What would you like to exclude?

FILE TYPE	LOCATION	
<input checked="" type="checkbox"/> Videos	custom	<a href="#">Edit</a>

[See file types](#)

Videos includes the following extensions:

.3g2, .dif, .m4v, .mpeg, .qts, .swf, .3gp2, .dv, .m75, .mpg, .rm, .wm, .3gpp, .flc, .mlv, .mps, .rmvb, .wmd, .amc, .fl, .mov, .mswmm, .rts, .wmv, .asf, .lrf, .mp2v, .mpv2, .rtsp, .wmz, .asx, .m1v, .mp4, .nsv, .rv, ...

Which will be excluded from protection in the following location:

C:\Users\UserName

Click Edit for full details.

Scan files now

- There are some default exclusions which cannot be overridden. For example, on Windows, system files and files and folders marked with an offline attribute are not backed up. On



macOS, block devices are not backed up. On both operating systems, .tmp files are not backed up. Contact your administrator for a full list of excluded files.

- If you are using a newer version of a OneDrive client on a macOS (Version 22.002.0103.0004 and later), files that appear as cloud only are not backed up by Carbonite Endpoint. OneDrive files that are stored locally are backed up on all macOS OneDrive versions.
- Your administrator limits the size of the files that are backed up. For example, if the administrator sets the maximum file size to 10 GB, then files included in a backup rule that are larger than 10 GB are not backed up.

Once you have configured your protection, you can wait until the next scheduled scan or you can click **Scan files now** on the **Protect** page or on the **Home** page. If you manually scan, the timing of your next scheduled scan is reset.



Starting with macOS 10.14 Mojave, the operating system includes a security feature called Full Disk Access (FDA) which blocks applications from accessing specific locations. This may prevent Carbonite Endpoint from backing up and restoring files, such as Apple Mail, Photos, Calendar, and so on. In order to back up and restore these files, you must enable Full Disk Access for Carbonite Endpoint.

#### **Enable Full Disk Access on a macOS 12, 11, 10.15 or 10.14 device**

1. Under the Apple icon, click **System Preferences, Security & Privacy**, and on the **Privacy** tab, select **Full Disk Access**.
2. If the padlock icon is locked, click the icon and enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
3. Click **Add an application** (the plus icon), click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.

#### **Enable Full Disk Access on a macOS 13 device**

1. Under the Apple icon, click **System Settings, Privacy & Security**, and select **Full Disk Access**.
  2. Click the plus icon.
  3. In the Privacy & Security box, enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
  4. Click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
-

# Configure hybrid protection

Go to the **Protect** tab. If this tab is not visible, your administrator is controlling protection and this section is not applicable to you.

A self-managed protection configuration is indicated by a table under the **Protect** tab that has check boxes on the left side of each table row. See *Configure self-managed protection* on page 14 for details. If the table does not have check boxes on the left side of each table row, you have a hybrid protection configuration. Use this section to configure your hybrid protection. Note that this section describes the optional process of including or excluding additional files, in addition to those configured by your administrator. If you do not make any modifications, you will still be protected using your administrator-defined rules.

The **Protect** tab is divided into two sections.

- **What would you like to protect**—This section contains backup rules that define the files to include in your backup.
- **What would you like to exclude**—This section contains exclusion rules that define the files to exclude from the backup.

The include and exclude sections are defined by a file type and a location. The file type can be pre-defined (all files, documents, email files, music and audio files, photos and images, or videos), or it can be a custom file type that you create. The location can be one specific location or multiple locations.



If you do not see the table of available items in either the protection or exclusions sections, click **See file types**.

What would you like to protect?		
FILE TYPE	LOCATION	
All Files	custom	<a href="#">Edit</a>
Documents	custom	<a href="#">Edit</a>
Email Files	custom	<a href="#">Edit</a>
Music & Audio	none defined	<a href="#">Edit</a>
Photos & Images	none defined	<a href="#">Edit</a>
Specific file types	none defined	<a href="#">Edit</a>
Videos	none defined	<a href="#">Edit</a>
<a href="#">+ Add a file type and location...</a>		

1. You may be able to see what your administrator has already configured by hovering over a **File Type** or **Location** in a row in the protect or exclude table. The tooltip displays the types of files that are included or excluded and the location the inclusion or exclusion is applied to. Keep in mind the following for the hover text.
  - User-created rules, if any exist, are displayed first.
  - Administrator-created rules are displayed after user rules.
  - A maximum of three rules are displayed in the hover text.
  - An ellipsis (...) indicates additional rules that are not displayed in the hover text.

2. If you want to view all of the rules for a file type or add additional locations to a file type, click **Edit**. The defined **Administrator Rules** display at the bottom of the page.
  - a. Identify the location.
    - **Add a specific location**—Click **Add a specific location**, select a volume or folder, and click **OK**. The location is included or excluded recursively, meaning the rule is automatically applied to the subfolders of the specified path (unless another rule exists for a subfolder). Consider the following when adding rules.
      - If your administrator has already defined a rule, you do not need to define the same rule.
      - If your rule conflicts with an administrator rule, you may or may not be able to save your rule, depending on whether your administrator allows overrides of the administrator rule. See the **Allow Override** column in the **Administrator rules** table. If overrides are allowed, your rule will take precedence over administrator rules. If overrides are not allowed, you cannot create a rule that conflicts with an administrator rule.
  - b. If you must remove one of the locations you defined, click **Remove**.
  - c. Click **Save** to save the modified rule.
3. If you want to create your own file types to include or exclude, click **Add a file type and location**. (If the link is not visible, click **See file types** to expand the table.)
  - a. Specify the details for the rule.

The screenshot shows a web form titled 'Protect > Add file type'. It has three main sections: 'File type' with a text input field containing 'Descriptive name for file types'; 'File extension details' with a text input field containing 'doc.docx'; and 'File type location' with a text input field containing 'C:\Folder1\Folder2'. To the right of the 'File type location' section are two links: 'Add a specific location' and 'All internal hard drives'. At the bottom right of the form is a 'Remove' link.

- **File type**—Specify a unique and descriptive name for the types of files you want to include or exclude.
- **File extension details**—Specify the file extensions you want to include or exclude. If you are specifying more than one extension, separate them with a space. Do not use periods, commas, asterisks, or any other characters specified in the console as invalid.
- **File type location**—Specify the location to look for these types of files. The location will be included or excluded recursively, meaning the rule is automatically applied to the subfolders of the specified path (unless another rule exists for a

subfolder).

- **Add a specific location**—Click **Add a specific location**, select a volume or folder, and click **OK**. Repeat this step to add multiple locations. Review the caveats below to understand how multiple rules interact with one another.
  - **All internal hard drives**—Click **All internal hard drives** to select all hard drives without having to enter them individually. Keep in mind that any custom locations you may have already specified are removed if you select this option.
- b. If you must remove a location, click **Remove**.
- c. Click **Save** to save your rule.



If you want to delete a custom rule, go back to **Edit** and click **Delete set**.

Consider the following when defining and selecting your rules.

- A rule for a file type takes precedence over a rule for **All Files**.
- In the case of multiple rules, files use the rule that is closest in the folder structure to them. In the following example, all files and folders under My Documents (which is C:\Users\UserName) will be backed up (the first rule). However, video files will be excluded from C:\Users\UserName and its subfolders (the third rule), except the videos located in C:\Users\UserName\Folder1\Folder2 and its subfolders will be included (the second rule).

The screenshot shows the 'What would you like to protect?' window. It has two main sections: 'What would you like to protect?' and 'What would you like to exclude?'. Each section contains a table with 'FILE TYPE' and 'LOCATION' columns. In the 'protect' section, 'All Files' and 'Videos' are listed with 'custom' locations. In the 'exclude' section, 'Videos' is listed with 'custom' location. A pop-up box titled 'Videos includes the following extensions:' lists various video file formats. Another box titled 'Which will be protected in the following location:' shows 'C:\Users\UserName\Folder1\Folder2'. A third box titled 'Which will be excluded from protection in the following location:' shows 'C:\Users\UserName'. A 'Scan files now' button is at the bottom right.

FILE TYPE	LOCATION
All Files	custom
Videos	custom

**What would you like to exclude?**

FILE TYPE	LOCATION
Videos	custom

- There are some default exclusions which cannot be overridden. For example, on Windows, system files and files and folders marked with an offline attribute are not backed up. On macOS, block devices are not backed up. On both operating systems, .tmp files are not backed up. Contact your administrator for a full list of excluded files.
- If you are using a newer version of a OneDrive client on a macOS (Version 22.002.0103.0004 and later), files that appear as cloud only are not backed up by Carbonite Endpoint. OneDrive files that are stored locally are backed up on all macOS OneDrive versions.

- Your administrator limits the size of the files that are backed up. For example, if the administrator sets the maximum file size to 10 GB, then files included in a backup rule that are larger than 10 GB are not backed up.

Once you have configured your protection, you can wait until the next scheduled scan or you can click **Scan files now** on the **Protect** page or on the **Home** page. If you manually scan, the timing of your next scheduled scan is reset.



Starting with macOS 10.14 Mojave, the operating system includes a security feature called Full Disk Access (FDA) which blocks applications from accessing specific locations. This may prevent Carbonite Endpoint from backing up and restoring files, such as Apple Mail, Photos, Calendar, and so on. In order to back up and restore these files, you must enable Full Disk Access for Carbonite Endpoint.

#### **Enable Full Disk Access on a macOS 12, 11, 10.15 or 10.14 device**

1. Under the Apple icon, click **System Preferences, Security & Privacy**, and on the **Privacy** tab, select **Full Disk Access**.
2. If the padlock icon is locked, click the icon and enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
3. Click **Add an application** (the plus icon), click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.

#### **Enable Full Disk Access on a macOS 13 device**

1. Under the Apple icon, click **System Settings, Privacy & Security**, and select **Full Disk Access**.
  2. Click the plus icon.
  3. In the Privacy & Security box, enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
  4. Click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
-

# Configure the protection settings

The default protection settings are configured by your administrator. You may or may not be able to override the defaults, depending on the access your administrator has granted. Use the following steps to configure the protection settings.

1. Click **Settings** at the bottom left of the console.
2. Configure your protection settings as required.

The screenshot shows a 'Settings' dialog box with three main sections: 'Backup Frequency', 'Backup Scheduling', and 'Network Utilization'.  
- **Backup Frequency**: A dropdown menu set to '15 minutes (recommended)'.  
- **Backup Scheduling**: A checkbox for 'Enable backup scheduling' is unchecked. Below it are time pickers for 'Start Time' (11:00 PM) and 'End Time' (05:00 AM).  
- **Network Utilization**: Two radio buttons; 'Use reduced network bandwidth for minimal impact on other applications (recommended)' is selected.  
At the bottom, there is a 'Proxy settings' button on the left and 'Cancel' and 'OK' buttons on the right.

- **Backup Frequency**—Set the time interval between scans. Scans occur independently of file processing and uploading. The next scan will start even if a previous scan has not completed its processing and uploading. If you manually scan before the next scheduled scan is set to run, the next scheduled scan time is reset.
- **Backup Scheduling**—Enable this option if you want to limit the time frame for scans. Setting a **Start Time** and **End Time** ensures that scans only occur between those times. Consider the following when configuring and using a schedule.
  - The difference between the two times must be at least one hour.
  - If the difference between the two times is smaller than the **Backup Frequency**, the scan will only run once when the backup schedule begins.
  - If the difference between the two times is larger than the **Backup Frequency**, the scan will run when the backup schedule begins and then run again at each specified interval until the backup schedule ends.
  - All scans that start before the end of the schedule will complete, even if the end of the schedule is reached before the scan is complete.
  - You can start a manual scan at any time by clicking **Scan files now** on the **Home** page or **Protect** page. Performing a manual scan resets the next scheduled scan time.
- **Network Utilization**—Select how much of the available network Carbonite Endpoint should use for backups. (This setting does not apply when restoring.)
  - **Use reduced network bandwidth for minimal impact on other applications**—Select this option to use only a portion of the network for backup data. Your administrator controls the upload rate. This option reduces the impact on other

applications running on your device, but slows down the data transfer.

- **Use all available network bandwidth**—Select this option to use all available network bandwidth for backup data. This option transfers the data as quickly as possible. You may want to use this option temporarily, for example during the initial backup or if you expect a large data change.

3. If you need to configure a proxy server to connect to the Internet, click **Proxy settings**.

- **No proxy**—Select this option if you do not need a proxy server to connect to the Internet.
- **Automatically detect settings**—Select this option to allow Carbonite Endpoint to automatically detect your proxy server configuration.
- **Specify the server and port**—Select this option if you want to specify the server (by name or IP address) and port number to use.
- **Use automatic configuration script**—Specify this option if you want to specify a server (by URL) that contains a proxy configuration script to use.
- **Proxy authentication**—If your proxy server requires authentication, specify the access credentials.

After you have configured your proxy server settings, click **Save**.

4. When your protection settings are complete, click **OK**.

# Restore files

You can restore your protected files from the vault. This can be helpful if you accidentally deleted a file, require an older version of a file, or need all of your files because your computer crashed or you received a new computer.

There are two ways to restore files:

- *Restore using the Carbonite Endpoint console* on page 25—You can restore a volume, folders, or files from the **Restore** page in the Carbonite Endpoint console. You can choose from the most recent version or a previous version. If you cannot find the Carbonite Endpoint console, contact your administrator.
- *Restore files using the web retrieval site* on page 28—You can restore the most recent version of a file using the web retrieval site. If you do not have permission to access the web retrieval site, you can only restore files using the Carbonite Endpoint console.

If you do not want to restore your own files, your administrator can also restore files for you.



# Restore using the Carbonite Endpoint console

You can restore a volume, folders, or files from the **Restore** page in the Carbonite Endpoint console. You can choose from the most recent version or a previous version. This may be helpful if you accidentally deleted a file, require an older version of a file, or if you need all of your files because your computer crashed or you received a new computer.

Your administrator can also restore files for you.

If you cannot find the Carbonite Endpoint console, contact your administrator.

1. Go to the **Restore** page.



Carbonite Endpoint may display a message asking you if you want to restore from a previous installation. If you select **Yes**, the files backed up with the most recent previous version (not an older previous version or the currently installed version) are automatically selected. See the **Restore point** description below for more information.

2. Select the volume, folder, or file that you want to restore in the table. Use the breadcrumb links above the table to move back up the folder tree.

Select files to restore

[C:](#) > [Folder1](#) > [Folder2](#) > [Folder3](#)

☒ Include deleted files

Search for files and folders

NAME	SIZE	DATE MODIFIED	LAST BACKUP	DELETED
File1.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File2.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File3.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	Today at 9:44 AM
File4.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File5.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File6.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File7.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File8.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	

Consider the following when using the table.

- You can select multiple items by using the Shift and Ctrl keys.
- Use the search box to locate specific items in multiple locations.
- Enable **Include deleted files** to view items that have been deleted from your device but are still on the vault. This option also displays files that are still on the vault that were once included in your backup rules but are now removed from the backup rules.



Files that were being protected and were renamed or moved are treated as deleted files. You will see the original file name or file location when you show deleted files.

- To display only the volumes, folders, and files protected at a specific date and time, click **Restore point** above the search box. This option lets you restore a previous version of a file.
  - **Most recent**—This option restores the most recent version that was backed up.
  - **Include files backed up at this time**—Select a date and time from the calendar and clock to restore the version of the file from that date and time. The file must have existed at the backup date and time and must still exist on the vault. Keep in mind, the date and time indicates when the file was backed up, and this may not be the same as the date and time when the file was saved.
  - **Select Today**—Click this option to use the current date and time. This is equivalent to the **Most recent** option that was the default.
  - **Or, select a previous install**—Select the installation date and time associated with the files you want to restore.
    - **Restore from current backup**—This option uses the files backed up by the current installation. Files that were backed up before this version was installed will not be listed in the table.
    - **Date and time**—If you had previous versions of Carbonite Endpoint installed and then uninstalled it, the previous versions will be listed by the uninstall date and time. If you select a previous installation, files that were backed up while this version was running will be available for restore, if they still exist on the vault.
- 3. Click **Next** to continue.
- 4. Review the **Restore summary** and select your restore settings as required.

**Confirm your restore settings**

---

**Restore summary**

3 files (57 Bytes) from Today at 9:49 AM Deleted files included in this restore

---

**Restore location**

Restore to:

☒ New location:  [Browse](#)

☐ Original location

---

**Name conflict**

If file exists:

☒ Create a new file with appended file name (don't delete existing file)

☐ Overwrite existing file (delete existing file)

- **Restore location**—Select where you want to restore the files.
  - **New location**—Select this option and specify an existing volume or folder where you want to restore the files.
  - **Original location**—Select this option to restore the files back to their original location, which is the location where they existed when they were backed up.



Before restoring files, whether you are restoring to the original location or a different location, make sure you have enough free space for the amount of data being restored. In most cases, the free space must be at least as large as the amount of data you are restoring. In some unique situations, such as restoring a single, large, non-compressible file, you may require free space that is at least



two times as large as the file you are restoring so that the non-compressed blocks can be downloaded and the final file created.

---

- **Name conflict**—Specify the method to resolve file name conflicts.
  - **Create a new file with appended file name**—If a file with the same name already exists in the specified **Restore location**, leave the existing file and restore the backup file using a new file name. The new file name will have .restored\* inserted between the file name and the extension, where \* is an incrementing number if the same restored file name already exists. For example, if you backed up File.doc , the restored file name will be File.restored.doc. If you restored that file again, the second restored file name will be File.restored2.doc. Restoring a third time would create a file named File.restored3.doc and so on.
  - **Overwrite existing file**—If a file with the same name already exists in the specified **Restore location**, that file will be overwritten by the restored file.
- 5. If you want to go back and view the files you are restoring, click **Back**.
- 6. When you are ready to begin the restoration, click **Restore**.

# Restore files using the web retrieval site

You can restore the most recent version of a file using the web retrieval site. If you do not have permission to access the web retrieval site, you can only restore files using the Carbonite Endpoint console. See *Restore using the Carbonite Endpoint console* on page 25. Alternatively, your administrator can restore files for you.

1. Obtain the URL for the web retrieval site from your administrator, if you do not already have it.
2. Open a web browser and enter the web retrieval site URL in the address bar.

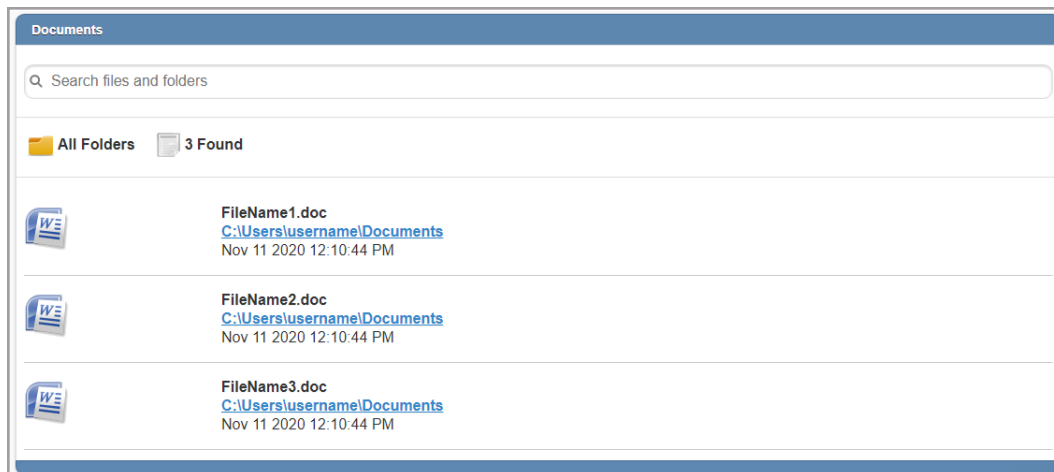


If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookie preferences are saved for a year in the browser, unless you clear your cookies.

3. On the login page, type your email address and password and click **Login**.

If you are prompted for an authentication code, enter an authentication code from your email or third-party authenticator app. For more information, see *Log in to the web retrieval site with two-factor authentication* on page 29.

4. Select your device from the list of devices.
5. Enter the name, or part of the name, of the file you want to restore in the search field. Be as specific as possible because the file list is limited to 20 files. If more than 20 files match your search, you may not see the file you want to restore. You can also use the search categories to narrow the file list, however the list is still limited to 20 files. You may still need to add the name, or part of the name, of the file in the search field.



To return to the previous page, click the curved arrow in the upper left corner, above the file list.

6. Click on the file you want to restore.

7. Confirm in the file details that it is the file you want to restore, then click **Download**. The file is automatically downloaded to the default download location on the computer you are using.
8. Repeat these steps for any other files you want to restore.
9. When you are finished, click the X in the upper right corner, above the file list, to log out.

## Log in to the web retrieval site with two-factor authentication

Two-factor authentication (2FA), also called multi-factor authentication (MFA), provides increased security for your data. When 2FA is enforced, you must enter an authentication code when you log in to the web access site to restore files.

You can receive an authentication code using two methods:

- **Email**—You can receive an authentication code in an email. This is the default 2FA method.
- **Mobile authenticator**—If you set up a mobile authenticator, you can obtain an authentication code from a third-party mobile authentication app, such as LastPass Authenticator, Microsoft Authenticator, or Google Authenticator, on your Android or iOS device. If you obtain codes from a mobile authenticator, you can also request authentication codes by email, if required. For more information, see *Set up or remove a mobile authenticator* on page 30.

If 2FA is not enforced, you can log in to the web retrieval site without entering an authentication code. If your company uses SSO (single sign-on), 2FA is disabled and you log in using the specified SSO method.

## Log in to the web retrieval site with an emailed authentication code:

1. Obtain the URL for the web retrieval site from your administrator, if you do not already have it.
2. Open a web browser and enter the web retrieval site URL in the address bar.



If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookie preferences are saved for a year in the browser, unless you clear your cookies.

---

3. On the login page, enter your email address and password, and click **Login**.

A message prompts you for an authentication code from your email.

4. Check your email for a message with an authentication code.

Make sure that Carbonite Endpoint emails are not blocked by spam filters or any other email blocking technology.

Emailed authentication codes are valid for 5 minutes. If you do not enter the code within that time frame, you must request a new code.

5. Enter the authentication code on the web retrieval site page, and click **Validate**.

A message asks if you want to set up a third-party authenticator. If you want to set up a mobile authenticator, click the link to open the **Security Settings** dialog box. For more information, see *Set up or remove a mobile authenticator* on page 30. If you do not want to set up a mobile authenticator, click the link to go to the home page.

## Log in to the web retrieval with a code from a mobile authenticator:

1. Obtain the URL for the web retrieval site from your administrator, if you do not already have it.
2. Open a web browser and enter the web retrieval site URL in the address bar.



If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookie preferences are saved for a year in the browser, unless you clear your cookies.

---

3. On the login page, enter your email address and password, and click **Login**.

A message prompts you for an authentication code from your mobile authenticator app.

4. Check the authenticator app for an authentication code.
5. Enter the authentication code on the web retrieval site page, and click **Validate**.

If you cannot obtain an authentication code from the authenticator app, click **Send new authentication code by email** to log in using an emailed authentication code.

## Set up or remove a mobile authenticator

When two-factor authentication (2FA) is enforced, you must enter an authentication code when you log in to the web retrieval site. See *Log in to the web retrieval site with two-factor authentication* on page 29.

By default, users receive authentication codes by email. If you set up a mobile authenticator, you can also obtain authentication codes from a third-party mobile authentication app on your Android or iOS device. You can set up a mobile authenticator if:

- 2FA is enforced for your company and enabled for your user.
- You have a mobile authentication app, such as LastPass Authenticator, Microsoft Authenticator, or Google Authenticator, installed on your Android or iOS device.

You can also remove a mobile authenticator from your account. If you remove a mobile authenticator, you must receive an authentication code by email when you next log in. System administrators can also remove users' mobile authenticators.

## Set up a mobile authenticator:

1. Do one of the following:
  - When logged in to the web retrieval site, click the gear icon at the top right corner of the page.
  - Log in using an emailed authentication code. See *Log in to the web retrieval site with two-factor authentication* on page 29. A message asks whether you would like to configure a third-party authenticator on your account. Click **Yes, take me to my security settings**.
2. Using a mobile authentication app on your Android or iOS device, scan the QR code shown on the page.

If you cannot to scan the code, click the **Can't scan the QR code?** link to display the key and enter the key manually.
3. Check the authenticator app for an authentication code. Enter the code and click **Save**.

A message indicates that an authenticator was successfully registered to your account.
4. Click **Close**.

## Remove a mobile authenticator:

1. When logged in to the web retrieval site, click the gear at the top right of the page.
2. Click **Remove authenticator**.
3. Check your email for a message with an authentication code.

Emailed authentication codes are valid for 5 minutes. If you do not enter the code within that time frame, you must request a new code.
4. Enter the authentication code in the Security Settings dialog box, and click **Remove**.

The mobile authenticator is removed. You must enter an emailed authentication code when you next log in to the dashboard.
5. Click **Close**.

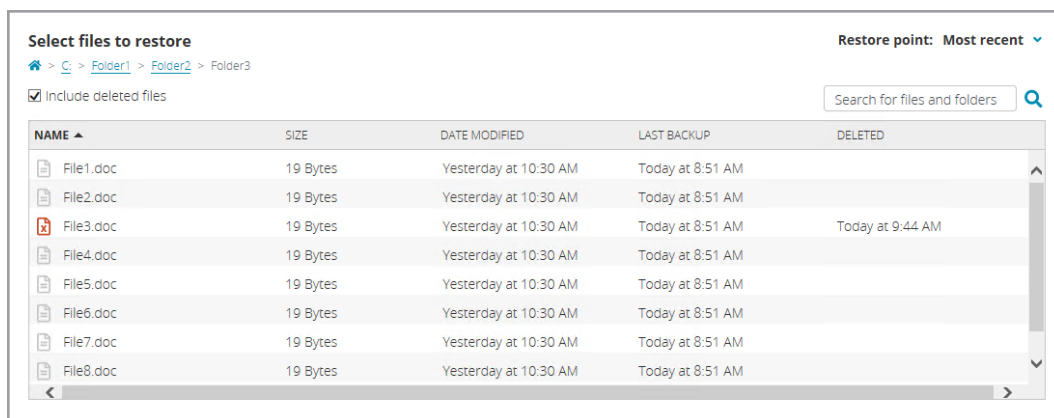
# Delete files on the vault

You can delete backed up files on the vault if your administrator has granted you access (indicated by a **Vault erase** button on the **Restore** page). Consider the following caveats if you want to delete files on the vault.

- If a file is deleted on the vault, all versions of that file are deleted.
- Files deleted on the vault cannot be restored.
- Files are deleted only on the vault and are not removed from your device.
- If you delete files that are included in an active backup rule, the files are backed up again during the next scan. If you no longer want to include the file in the backup, change your protection configuration. See *Configure self-managed protection* on page 14 or *Configure hybrid protection* on page 18 for details.

Use the following steps to delete files on the vault.

1. Go to the **Restore** page.
2. Select the volume, folder, or file that you want to delete. Use the breadcrumb links above the table to move back up the folder tree.



Select files to restore

Restore point: Most recent

> > C: > Folder1 > Folder2 > Folder3

☒ Include deleted files

Search for files and folders

NAME	SIZE	DATE MODIFIED	LAST BACKUP	DELETED
File1.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File2.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File3.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	Today at 9:44 AM
File4.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File5.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File6.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File7.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	
File8.doc	19 Bytes	Yesterday at 10:30 AM	Today at 8:51 AM	

Consider the following when using the table.

- You can select multiple items using the Shift and Ctrl keys.
- Use the search box to locate specific items in multiple locations.
- Enable **Include deleted files** to view items that have been deleted from your device but are still on the vault. When enabled, this option also displays files that are still on the vault that were once included in your backup rules but are now removed from the backup rules.



Files that were being protected and were renamed or moved are treated as deleted files. You will see the original file name or file location when you show deleted files.

- If you are deleting files on the vault, the **Restore point** option is not used. All versions of the files will be deleted.



3. Click **Vault erase**. If this button is not visible, your administrator has not granted you access to delete files on the vault.
4. Confirm you want to delete the files on the vault by clicking **Yes**.
5. When prompted, click **OK** after the vault erase request has been submitted.

You can confirm the success of the deletion on the **Home** page under **Recent Activity**.


# Resolve file issues

If you had an alert on the **Home** page and clicked **View file issues**, you will go to the **Issues** page. Review the issues in the list and decide how you want to handle them. Select **Include files in the list which have been marked as 'Stop Protecting'** if you want the list of issues to include files that you previously stopped protecting.

[Home](#) > [Issues](#)

**Issues**

☐ Include files in the list which have been marked as 'Stop Protecting'

FILE	ISSUE DATE ▲	ISSUE
 C:\Users\...uments\FileName.doc	Today at 1:10 PM	File too big - could not back it up

**Description**  
Review each issue and select an action. You can select multiple issues at one time.

Retry files

Stop protecting

Back

You can select an action for individual issues or select multiple issues at once and apply the same action to all of them.

- **Retry files**—Select this option if you want to retry the selected files. The files will be retried during the next scan.
- **Stop protecting**—Select this option if you want to stop protecting the selected files. Once protection is stopped, the file will be skipped in future scans.

If you want to start protecting a file that you have previously stopped protecting, locate it in the file list by enabling the include files marked as stop protecting, and then click **retry**. The file will be retried during the next scan.