Notices

Carbonite Endpoint User Guide, version 10.9, Tuesday, July 20, 2021

If you need technical assistance, you can contact CustomerCare. All basic configurations outlined in the online documentation will be supported through CustomerCare. 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 Carbonite, Inc.; 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.

Carbonite, Inc. and/or its affiliates and subsidiaries in the United States and/or other countries own/hold rights to certain trademarks, registered trademarks, and logos. Windows is a registered trademark of Microsoft. Mac is a registered trademark of Apple. 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.

© 2021 Carbonite, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>Get started</td>
<td>6</td>
</tr>
<tr>
<td>Requirements</td>
<td>7</td>
</tr>
<tr>
<td>Install Carbonite Endpoint</td>
<td>9</td>
</tr>
<tr>
<td>Console</td>
<td>12</td>
</tr>
<tr>
<td>Protection</td>
<td>14</td>
</tr>
<tr>
<td>Configure self-managed protection</td>
<td>15</td>
</tr>
<tr>
<td>Configure hybrid protection</td>
<td>19</td>
</tr>
<tr>
<td>Configure the protection settings</td>
<td>23</td>
</tr>
<tr>
<td>Restoration</td>
<td>25</td>
</tr>
<tr>
<td>Restore using the Carbonite Endpoint console</td>
<td>26</td>
</tr>
<tr>
<td>Restore using the web retrieval site</td>
<td>29</td>
</tr>
<tr>
<td>Delete files on the vault</td>
<td>30</td>
</tr>
<tr>
<td>Resolve file issues</td>
<td>32</td>
</tr>
</tbody>
</table>
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 7—Review this information to make sure your Windows or MacOS device meets the minimum requirements.
2. Install Carbonite Endpoint on page 9—If your administrator did not push Carbonite Endpoint to your device, you will need to install it manually.
3. Console on page 12—Review this section to familiarize yourself with the Carbonite Endpoint interface.
4. Protection on page 14—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 Restoration on page 25, or if you want to delete files on the vault see Delete files on the vault on page 30.
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 10
  - Windows 8.1
  - Windows 8
  - Windows 7

Windows Starter Editions are not supported.

- **MacOS operating system**—The following Mac OS operating systems are supported.
  - MacOS 11.0 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 grant Carbonite Endpoint access within Full Disk Access. Make sure you make the following change on a MacOS 10.14 or later 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), highlight **Applications** on the left, select Carbonite Endpoint from the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.
5. Restart the device.

- **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 will need to install it manually 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 being 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. If desired, deselect the options for the desktop shortcut and running the client after the installation. These option 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 get this URL from an email from your administrator.

• **Activation Code**—This is the activation code for the device. In most cases, you can get 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 23 for details.

13. Click **Next** to continue.

14. If you are reactivating a previously used device, you will be 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

The Carbonite Endpoint console is where you can protect and restore your files. 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.

By default, the console has three tabs, Home, Protect, and Restore, across the top right of the console that access the different areas of the application. Your view may vary depending on the access your administrator has granted. At the bottom left bottom you will see a Settings link to access protection settings and links to access console information and help. Towards the bottom right corner of the console, under the activity table, you will see a status message indicating if your device is connected to the vault.

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

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

![Console](image)

- **Status**—The top section shows the current status, for example, if your device is protected or unprotected or if it is in the process of backing up or restoring files. This section also notes when your next scheduled scan will be.

  If you want to start a manual backup scan immediately, click **Scan files now**. If you manually scan, the timing of your next scheduled scan will be reset.

  If you have any issues with your protection, you will see an **Alerts** box in the top section. If the alert has additional information, click the link to see the details. See **Resolve file issues** on page 32 for details.

- **Details**—The middle section shows if a backup or restore is actively occurring along with processing information. If it is blank, nothing is currently being scanned or processed.
- **Recent Activity**—The bottom section shows each individual protection scan or restore processing including when it occurred, the number of files backed up or restored, the status of the process, and the type of activity. If you want to see detailed information on the individual process, click **Details**. Other processing activity, for example after a device reset, may not have details available.

- **Protect**—This tab is where you configure the files you want to back up. See **Protection** on page 14 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 23 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 26 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.
Protection

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, you will not see a Protect tab. You will only see a Home and Restore tab. 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 15 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 letting you know 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 19 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 23 for details.
Configure self-managed protection

Go to the Protect tab. If you do not see this tab, you cannot control which files are and are not protected because your administrator has that control. In this case, this section is not applicable to you.

On the Protect tab, if you see a table with checkboxes at the left side of each table row, you have a self-managed configuration. Use this section to help configure your self-managed protection. If you have the Protect tab and the table does not have checkboxes at the left side of each table row, you have a hybrid configuration. See Configure hybrid protection on page 19 for details.

The Protect tab is divided into two sections.

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

1. Select any of the pre-defined file types and default locations for backup or exclusion by clicking the checkbox 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 see the details of the rule.
   b. Click **Add a specific location**, select a volume or folder, and click **OK**. The location will be included or excluded recursively, which means 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 each other.
   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 backup or exclude, use the following steps.
   a. Click **Add a file type and location**. (If you do not see that link, click **See file types** to expand the table and view the link to add a file type.)
   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 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, which means 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 each other.
c. If you need 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).

- There are some default exclusions which cannot be overridden. For example, on Windows, system files and files and folders marked with an offline attribute will not be backed up. On MacOS, block devices will not be backed up. On both operating systems, .tmp files will not be backed up. Contact your administrator for a full list of excluded files.
- Your administrator will limit large files from being 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 will not be 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 will be 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 grant Carbonite Endpoint access within Full Disk Access. Make sure you make the following change on a MacOS 10.14 or later 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), highlight **Applications** on the left, select Carbonite Endpoint from the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.
5. Restart the device.
Configure hybrid protection

Go to the Protect tab. If you do not see this tab, you cannot control which files are and are not protected because your administrator has that control. In this case, this section is not applicable to you.

On the Protect tab, if you see a table with checkboxes at the left side of each table row, you have a self-managed configuration. See Configure self-managed protection on page 15 for details. If you have the Protect tab and the table does not have checkboxes at the left side of each table row, you have a hybrid configuration. Use this section to help configure your hybrid protection. Keep in mind that this section is for the optional process of including or excluding additional files, beyond what your administrator has configured. 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 what files to include in your backup.
- **What would you like to exclude**—This section contains exclusion rules that define what 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.

<table>
<thead>
<tr>
<th>FILE TYPE</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Files</td>
<td>custom</td>
</tr>
<tr>
<td>Documents</td>
<td>custom</td>
</tr>
<tr>
<td>Email Files</td>
<td>custom</td>
</tr>
<tr>
<td>Music &amp; Audio</td>
<td>none defined</td>
</tr>
<tr>
<td>Photos &amp; Images</td>
<td>none defined</td>
</tr>
<tr>
<td>Specific file types</td>
<td>none defined</td>
</tr>
<tr>
<td>Videos</td>
<td>none defined</td>
</tr>
</tbody>
</table>

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 will show you the kinds 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, are displayed first.
   - Administrator created rules are displayed after user rules.
   - At most three rules are displayed in the hover text.
   - If you see an ellipsis (…), there are 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. At the bottom of the edit page, you will see the defined Administrator Rules.
a. Identify the location.
   - **Add a specific location**—Click **Add a specific location**, select a volume or folder, and click **OK**. The location will be included or excluded recursively, which means the rule is automatically applied to the subfolders of the specified path (unless another rule exists for a subfolder). Keep in mind the following when adding rules.
     - If your administrator has already defined a rule, there is no need for you 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 if 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 will not be able to create a rule that conflicts with an administrator rule.

   Repeat this step to add multiple locations. Review the caveats below to understand how multiple rules interact with each other.

   - **All internal hard drives**—Click **All internal hard drives** to quickly select all hard drives without having to enter them individually. Keep in mind that any custom locations you may have already specified will be removed if you select all hard drives. This option is not available if the **File type** is **All Files**.

b. If you need to 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 you do not see that link, click **See file types** to expand the table and view the link to add a file type and location.)
   a. Specify the details for the rule.

   ![File type interface](image)

   - **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, which means 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 each other.

- **All internal hard drives**—Click All internal hard drives to quickly select all hard drives without having to enter them individually. Keep in mind that any custom locations you may have already specified will be removed if you select all hard drives.

b. If you need to remove a location, click Remove.

c. Click Save to save your rule.

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).

- There are some default exclusions which cannot be overridden. For example, on Windows, system files and files and folders marked with an offline attribute will not be backed up. On MacOS, block devices will not be backed up. On both operating systems, .tmp files will not be backed up. Contact your administrator for a full list of excluded files.

- Your administrator will limit large files from being 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 will not be 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 will be 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 grant Carbonite Endpoint access within Full Disk Access. Make sure you make the following change on a MacOS 10.14 or later 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), highlight **Applications** on the left, select Carbonite Endpoint from the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.
5. Restart the device.
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. If you are able and so desire, you can modify these settings.

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

- **Backup Frequency**—Set the amount of time to wait between scans. The scans are independent of processing and uploading files. 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 timing of your next scheduled scan will be reset.
- **Backup Scheduling**—Enable this option if you want to limit when the scans occur. Set a **Start Time** and **End Time** and the scans will only occur between those times. Keep in mind the following when 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 frequency 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 inside or outside of the schedule by clicking **Scan files now** on the **Home** page or **Protect** page. If you manually scan, the timing of your next scheduled scan will be reset.
- **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 does not send the data as fast.
- **Use all available network bandwidth**—Select this option to use all available network bandwidth for backup data. This option will send 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 let Carbonite Endpoint 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 credentials to access the proxy server.

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

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

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

There are two ways you can restore files.

- *Restore using the Carbonite Endpoint console* on page 26—Using the Restore page in the Carbonite Endpoint console, you can restore a volume, folders, or files. You can choose from the most recent version or a previous version. If you cannot find the Carbonite Endpoint console, contact your administrator.

- *Restore using the web retrieval site* on page 29—Using the retrieval web site, you can restore the most recent version of a file. If your administrator has not granted you access to the web retrieval page, you can only restore files using the Carbonite Endpoint console.

If you do not want to use either of these methods, your administrator can also restore files for you.
Restore using the Carbonite Endpoint console

Using the Restore page in the Carbonite Endpoint console, you can restore a volume, folders, or files. You can choose from the most recent version or a previous version. This may be helpful if you accidentally deleted a file, need 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.

   If you were prompted when you clicked Restore if you want to restore from a previous installation and you selected Yes, the files backed up with the most recent previous version (not an older previous version or the current installed version) will automatically be selected. See the description about Restore point below.

2. In the table, drill-down and select the volume, folder, or file that you want to restore. Use the breadcrumb links above the table to go back up the folder tree.

Keep in mind 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. When enabled, this option also shows 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 show 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 will restore 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 is when the file was backed up, which 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.

<table>
<thead>
<tr>
<th>Confirm your restore settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore summary</strong></td>
</tr>
<tr>
<td>3 Folders (574 bytes) from Today at 9:48 AM</td>
</tr>
<tr>
<td><strong>Restore location</strong></td>
</tr>
<tr>
<td>New location: C:RestoreFolder</td>
</tr>
<tr>
<td><strong>Name conflict</strong></td>
</tr>
<tr>
<td>If file exists:</td>
</tr>
<tr>
<td>Create a new file with appended file name (don't delete existing file)</td>
</tr>
<tr>
<td>Overwrite existing file (delete existing file)</td>
</tr>
</tbody>
</table>

• **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 they existed when they were backed up.

---

Regardless of restoring to a new or original 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 need...
free space to be 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 how you want file name conflicts to be resolved.
  - **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 again would be 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 need to go back and see the files you are restoring, click **Back**.
6. When you are ready to being the restoration, click **Restore**.
Restore using the web retrieval site

Using the retrieval web site, you can restore the most recent version of a file. If your administrator has not granted you access to the web retrieval page, you can only restore files using the Carbonite Endpoint console.

Your administrator can also restore files for you.

1. If you do not already have it, get the URL for the web retrieval site from your administrator.
2. Go to the web retrieval site and log in.
3. Select your device from the list of devices.
4. 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.

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

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

If your administrator has granted you access, you can delete backed up files on the vault. You can tell if you have access if you see a Vault erase button when you go to the Restore page. Keep in mind 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 will be deleted.
- After a file is deleted on the vault, it cannot be restored.
- This process only removes files on the vault, not from your device.
- If the files you are deleting are included in an active backup rule, they will be backed up again during the next scan. If you no longer want to include that file in the backup, change your protection configuration. See Configure self-managed protection on page 15 or Configure hybrid protection on page 19 for details.

Use the following instructions to delete files on the vault.

1. Go to the Restore page.
2. In the table, drill-down and then select the volume, folder, or file that you want to delete. Use the breadcrumb links above the table to go back up the folder tree.

Keep in mind 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. When enabled, this option also shows 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 you do not see this button below the table, 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.

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.