CARBONITE

Carbonite Safe Server Backup

Handbook

Carbonite Safe Server Backup Manual for 6.x

What is Carbonite Safe Server Backup (CSSB)

Carbonite Safe Server Backup (CSSB) is a comprehensive backup solution for small and medium-sized businesses that need a disaster recovery solution for their Windows servers, desktops, laptops, and applications such as Microsoft Exchange, Exchange Online, SharePoint, Hyper-V and SQL Server. CSSB offers customers the ability to perform an image backup and a bare metal restore to a new or existing system.

Carbonite Safe Server Backup, available in our Safe Power and Ultimate plans, can recover anything from a single file to an entire system with the click of a button. So, whether you don't have an IT department or you *are* the IT department, you can rest easy knowing the data that powers your business is safe.

Plans and Pricing

Pricing information for our Carbonite Safe Backup Pro plans bundled with Carbonite Safe Server Backup is available on our [pricing page](#).

System Requirements

The current version of Carbonite Safe Server Backup is designed to support all versions of each Windows operating system listed below:

- Windows 7
- Windows Server 2008 R2
- Windows Small Business Server 2011
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

*Server core installations are not supported for any version of Windows.

If you are running a 32-bit operating system on Windows 7, 8/8.1 or Windows 10, the latest client version of CSSB will be 6.5.

If you are running Windows XP, Windows Vista, Windows Server 2003, or Windows Server 2008, the latest client version of CSSB will be 5.6

Hardware Requirements:

- Dual-core CPU
- 2GB of RAM or higher
- 10GB or more of disk space on the drive where CSSB is installed for CSSB's own program and configuration files.
    - Additionally, every disk that contains data to be backed up must have space for VSS snapshots. This space is known as shadowstorage. **At least 10%** of each disk should be dedicated to shadowstorage. CSSB will automatically create and assign shadowstorage to meet this requirement. You can read more about shadowstorage in [this Knowledge Base article](#).

Dependencies

- Amazon Corretto 8 (or higher) is required for full CSSB functionality.

   - Systems are required to run Corretto 8. For additional information about CSSB and its dependency on Corretto, please review this Knowledge Base article.

- Backups of Microsoft Exchange Server 2007 have additional requirements/dependencies:

   - Microsoft .NET Framework 4.0 must be installed on the machine where CSSB is installed.

   - PowerShell 2.0 or higher (part of the Windows Management Framework) must also be installed on the machine where CSSB is installed.

- The **Check Dependencies** option on the *Advanced* page can be used to verify if the proper dependencies are installed on the system.

Other Requirements

- Your system must also meet these requirements:

   - The language selected in the CSSB Installer and the CSSB program must match the Windows system locale.

   - The Remote Registry Service must be enabled before installation.

   - The Volume Shadow Copy Service (VSS) must be enabled. Although the Volume Shadow Service is enabled by default, it may have been turned off after Windows installation. To ensure that VSS is running:

      - Right-click the **My Computer** (or **Computer**) icon and choose **Manage** from the pop up menu.

      - Expand the *Services and Applications* tree and locate the **Volume Shadow Copy** Service. If it is not started, change the General Properties to make the *Startup Type* **Automatic**.

   - Carbonite Safe Server Backup must be installed and all CSSB operations must be performed as a user that has Administrator privileges.

   - Carbonite Safe Server Backup requires access to **TCP Ports 10080 and 10081**, which are the default ports used by CSSB for backup and restore operations.

      - Alternate ports can be specified by clicking the **Data Transferring and Networking** link (within the Global Settings section) on the Advanced page of the CSSB Enhanced Interface.

   - The Carbonite Server Cloud Controller requires access to port 10085. If port 10085 is not available, please refer to the Knowledge Base article entitled Changing the Default Port Used by the ZCBService for additional information.

   - CSSB depends on the Visual C++ Redistributable. VC++ must be installed and in working order on the system.

      - Errors that reference *MSVCP120.dll* indicate a damaged or corrupted Microsoft VC++ Redistributable. The systems administrator must repair or reinstall VC++ in order to resolve the errors.

Getting Started with Carbonite Safe Server Backup

Normally when using CSSB, you don't have to worry about creating new users or assigning computers. However, if you're also using the computer backup product, you will be able to manage your users/administrators and add/remove/assign computers to your account. If you'd like to do that as well, please use these instructions.

Creating a Carbonite Account

You can create your Carbonite account and install a 30-day free trial from the Carbonite website at https://www.carbonite.com/backup-software/safe-business-trial/.

On the trial page, you will be required to enter some information into the required fields below:

- **First Name:** This is the first name you would like registered with the account.
- **Last Name:** This is the last name you would like registered with the account.
- **Company Name:** This is the name of the company you are registering with Carbonite.
- **Phone:** This is a phone number that can be used if, for any reason, we need to contact you directly.
- **Email:** This is the email address that will be associated with your Carbonite account. Please ensure that you are typing in an address that you are able to access and receive emails from. This email address will be used to identify your account and will receive any password reset requests.
- **Password:** This is the password that will be associated with your Carbonite account.
- **Confirm Password:** This is to ensure that the password you have just entered above is the one you would like associated with your Carbonite account.

Once you have entered all the required the information and reviewed it, click **Submit** to proceed.

Once your account has been created, you will be taken to your Carbonite Dashboard. From this window, you will be able to schedule a free valet installation with one of our experts. You will have to download and import your cloud certificate to perform cloud backups.

Server Dashboard

Note: By default, your trial will be a Carbonite Safe Ultimate plan which will allow you to back up an unlimited number of computers and servers.

Valet Installation

After creating an account, you will be able to schedule a free valet installation from the Dashboard by clicking the **Click here to schedule your FREE valet installation** link. After entering all the required information pertaining to your Server Backup installation and submitting your request, a customer care representative will contact you to assist with the installation and setup of CSSB.

If you have already installed Carbonite Safe Server Backup on your computer, you may not see the valet installation link. If you require assistance configuring your software, we recommend contacting our Customer Care Team about scheduling an appointment.

Installation Through the Dashboard

If you choose to install Carbonite Safe Server Backup, navigate to https://account.carbonite.com and sign into your account with your email address and password.

Sign Into Your Account

Within the *Dashboard*, click the **Install Carbonite** button located under *I want to back up a Server.*

8
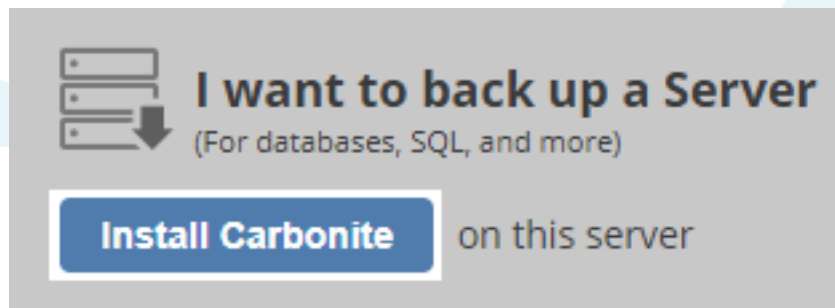
Select the correct operating system and click the **Download the installer** button to start the download. If you plan to perform cloud backups, you will be required to download and import your cloud certificate. Follow the on-screen instructions to proceed with the installation.

During the installation process, you will be required to select a password for the *CarboniteUser* user. CSSB automatically creates this user with administrator privileges, which is required for backup-related tasks. For additional information, please review this Knowledge Base article.

For additional information about the installation process, please review this Knowledge Base article.

Starting CSSB

After launching Carbonite Safe Server Backup for the first time, you will be presented with a Welcome to Carbonite Safe Server Backup window. On this screen, you will be able to perform the following actions:

- *Import My Cloud Certificate* – Clicking this button will direct you to your Carbonite account, where you will be able to download and import your cloud certificate.
- *Schedule a free valet install* – Clicking this link will direct you to the valet installation page.
- *Carbonite's Knowledge Base* – Clicking this link will direct you to our Knowledge Base located at https://support.carbonite.com.

Once the cloud certificate has been downloaded and imported, you will be given the choice to either start backing up or restoring data.

Click **Start backing up my server** to configure your first backup set.

Additional information will be provided in this document on how to configure backup sets and import existing backup sets.

- Not all backup types will be supported by the new Enhanced User Interface. For additional information about the backup types supported by the Classic User Interface (same UI as in CSSB 5.5), please review the information in this document pertaining to switching between the Enhanced and Classic UI.
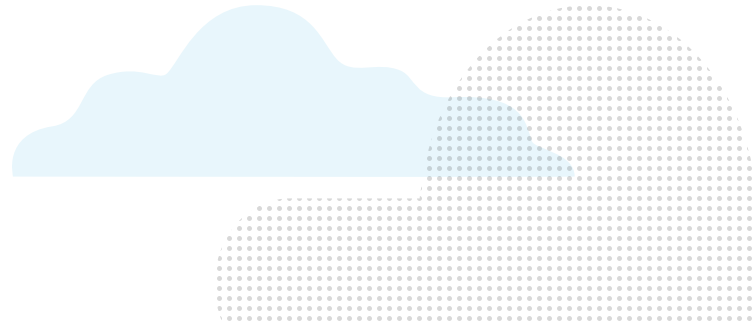
Server Dashboard

Backups on the cloud can be monitored using the Dashboard. You can view detailed reports on all current cloud backups for all computers under your account, install, reinstall Carbonite Safe Server Backup, and download your cloud certificate through the Dashboard. You can also manage users and administrators through the Dashboard. You can access the Dashboard by logging into your account at https://account.carbonite.com. Within the Dashboard, click the **Servers** tab to view a list of computers associated with a server backup.
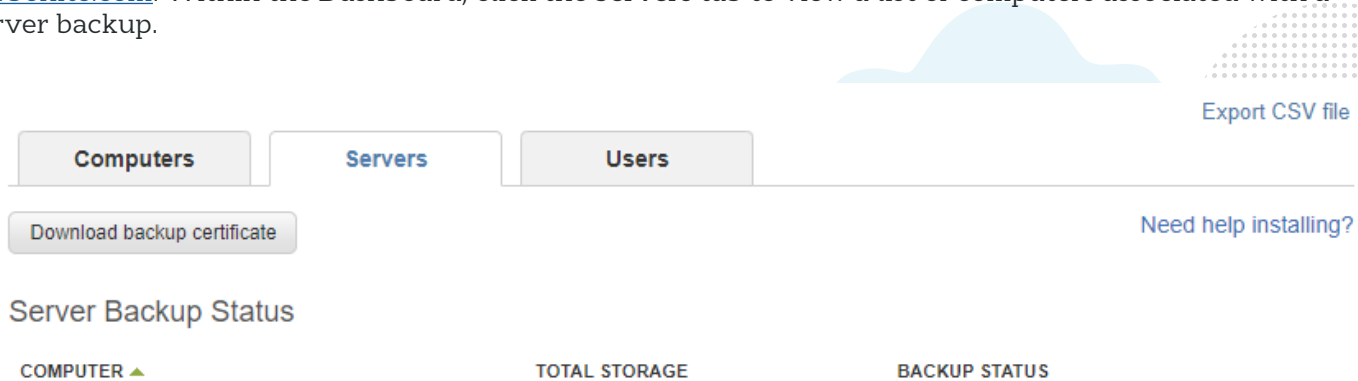
If you have installed CSSB on a computer/server and performed a backup run, the following information will be displayed:

- **Server backup status:** It shows detailed information about all the computers being backed up, listing the name of the computer(s), the amount of storage (in GB) and the percent of storage used by each computer, along with their backup status.
- **Backup runs:** It shows detailed information about all the backup runs associated with a server backup, listing the computer name(s), the backup set(s), the backup level (full, incremental, or differential), the date of the most recent activity for each backup run, the total storage (in GB) used by each backup run, and the backup status for that backup run.

Assistance Installing

If you require some assistance installing Carbonite Safe Server Backup on your computer, click the **Need help installing?** link.
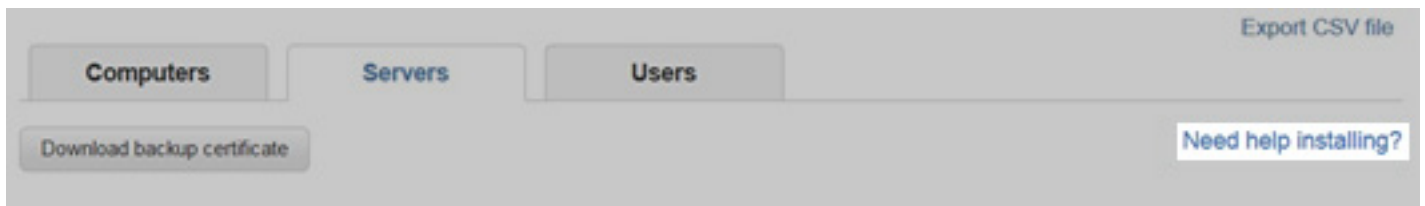
An *Installing Carbonite Safe Server Backup* window will appear.
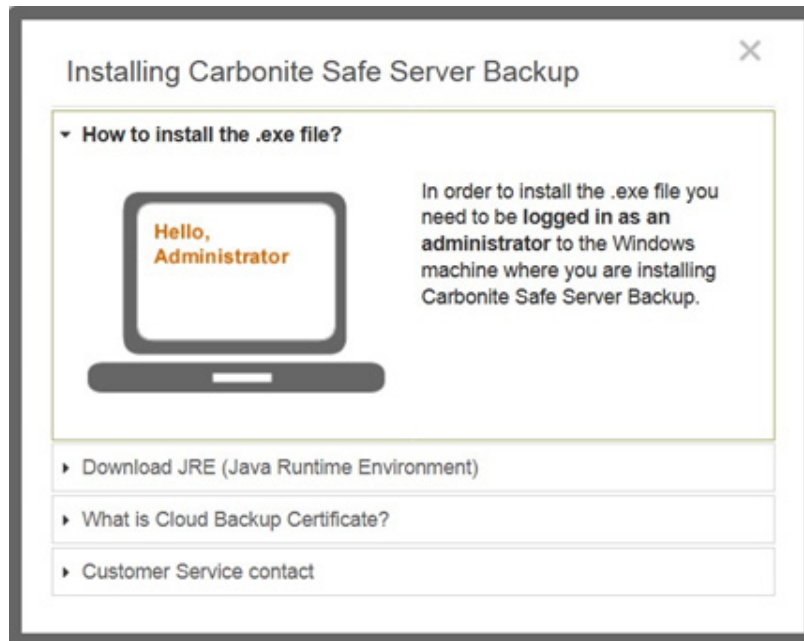
Within this screen, the following sections are displayed:

- **How to install the .exe file** – In order to install and run the .exe file, you need to be logged in as an administrator on the Windows machine where CSSB is being installed.
- **What is the Cloud Backup Certificate** - A description of the cloud backup certificate and a link to download it is provided.
- **Customer Service contact** - The Customer Care phone number and the hours of operations are provided. For additional information about the Server Dashboard, please view this Knowledge Base article.

Cloud Storage Quota

All Carbonite Safe Server Backup plans include a set amount of cloud storage. If you exceed your storage quota, you must purchase additional storage or delete some of your existing backups to continue uploading data to the cloud.

To delete backup runs for a specific backup set, within the Dashboard, place a checkmark next to each backup run you wish to delete. Once a backup run has been selected, a **Delete backup runs** button will appear. Click it to proceed.

Note: You can also select multiple backup runs for deletion by placing a checkmark in the box next to the **COMPUTER** column.

A confirmation window will appear. Click **Yes, delete** to confirm the deletion.

This action cannot be undone and deleted backup runs cannot be recovered. Deleting a full backup will also delete all associated incremental and differential backups.

Once the backup run has been deleted, it will be removed from the account Dashboard.

Server Backup Status

COMPUTER	TOTAL STORAGE		BACKUP STATUS
OPT745-00024	5.1 GB	0%	OK (Last backup Apr 12, 2017)
E7470-05656	.01 GB	0%	OK (Last backup Apr 12, 2017)

Backup runs

Backup runs include all full, incremental, and differential backups for your backup sets. When deleting
backups, we recommend deleting full cycles with all associated child (incremental or differential) backups.

Delete backup runs

	COMPUTER	SET	BACKUP LEVEL	LAST ACTIVITY ▾	TOTAL STORAGE	STATUS
☐	OPT745-00024	Test Windows Backup Set	Incremental	Apr 12, 2017 20:41:20	.01 GB	Success
	E7470-05656	Backup set 1	Incremental	Apr 12, 2017 20:41:01	.01 GB	Success
	OPT745-00024	Backup Set 1	Incremental	Apr 12, 2017 20:40:44	.01 GB	Success
	OPT745-00024	Test Windows Backup Set	Incremental	Apr 11, 2017 20:42:25	.01 GB	Success
	OPT745-00024	Backup Set 1	Incremental	Apr 11, 2017 20:42:09	.01 GB	Success
	E7470-05656	Backup set 1	Incremental	Apr 11, 2017 20:41:00	.01 GB	Success
☐	OPT745-00024	Test Windows Backup Set	Full	Apr 10, 2017 21:05:51	.75 GB	Success
☐	OPT745-00024	Backup Set 1	Full	Apr 10, 2017 21:02:11	.02 GB	Success
	OPT745-00024	Windows File System	Incremental	Apr 10, 2017 20:41:38	.01 GB	Success

For additional information about managing your storage quota, please review this Knowledge Base article.

Managing Administrators

With the Carbonite **Safe Power** and **Safe Ultimate** plans, you can manage users and administrators from
your Carbonite account. There is no limit to the number of users or administrators that you can add. An
administrator has more functionality than a user and can manage other users and administrators within the
account. You can also remove any users or other administrators from your account, excluding the current
Billing Owner.

For additional information about managing users and administrators, please view this Knowledge Base
article.

15

Purchasing a Subscription

You can purchase a subscription to Carbonite Safe Server Backup through the Dashboard. Your purchase will also include free valet installation up to 30 days from the date of purchase for an unlimited number of servers.

For additional information about purchasing, please review this Knowledge Base article.

Adding Additional Storage

You can add additional storage to your Carbonite Safe Server account through your Dashboard at any time, after you purchase a subscription. The price of the additional storage will be prorated based on the amount of time remaining in your current subscription.

For additional information about adding cloud storage, please review this Knowledge Base article.

Upgrading Your Subscription

You can upgrade your Carbonite Safe Server Backup subscription at any time. When you upgrade your plan, you will receive a credit towards your upgraded subscription if there is time remaining on your current subscription. You will also be able to immediately take advantage of all the features available with your new plan.

For additional information about upgrading, please review this Knowledge Base article.

The Backup Dashboard

The task of managing your backup involves answering four key questions:

- What would you like to back up?
- Where would you like to back up?
- How would you like to back up?
- When would you like to back up?

A CSSB backup is made up of your answers to the above four questions.

Creating a File System Backup Set

A backup set defines the parameters for backing up a group of directories or an application. You can only select one backup type for each backup set. For example, you cannot back up an Exchange server and Windows System state in the same backup set. Instead, you must create a new backup set for each type of backup.

To create a new backup set, launch Carbonite Safe Server Backup. After scanning your computer/server, you will be presented with recommendations for creating backup sets, based on the data and applications detected on your system. Select the File System backup set and click **Continue**.
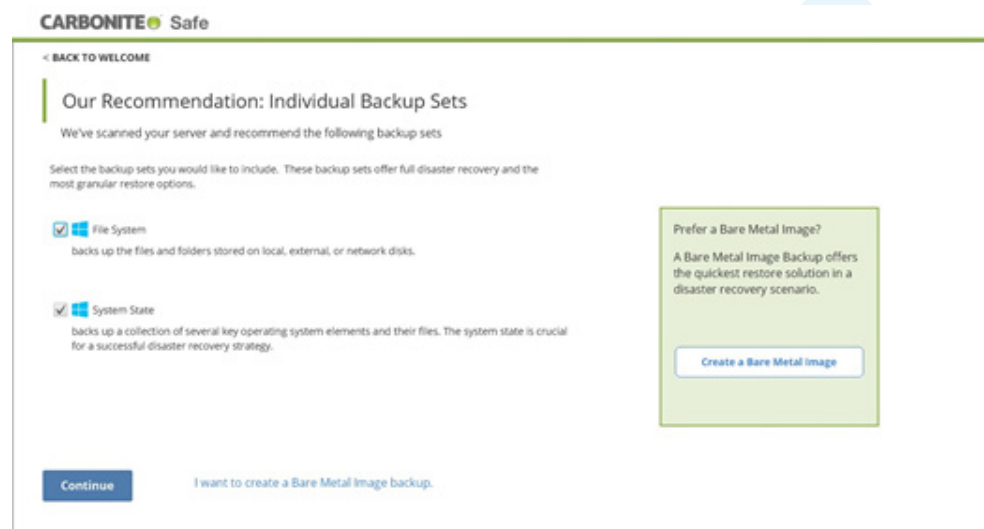
In the above example, CSSB recommended that you also perform a System State backup. You also have the option of performing a Bare Metal Image backup, which offers the quickest restore solution in a disaster recovery scenario. Please review this Knowledge Base article for instructions on how to configure these backup sets, to ensure you have a complete disaster recovery solution for your system.

> Not all backup types will be supported by the new Enhanced User Interface. For additional information about the backup types supported by the Classic User Interface (same UI as in CSSB 5.3), please review this Knowledge Base article.

On the next screen, you will be able to choose your local and cloud backup locations.

17
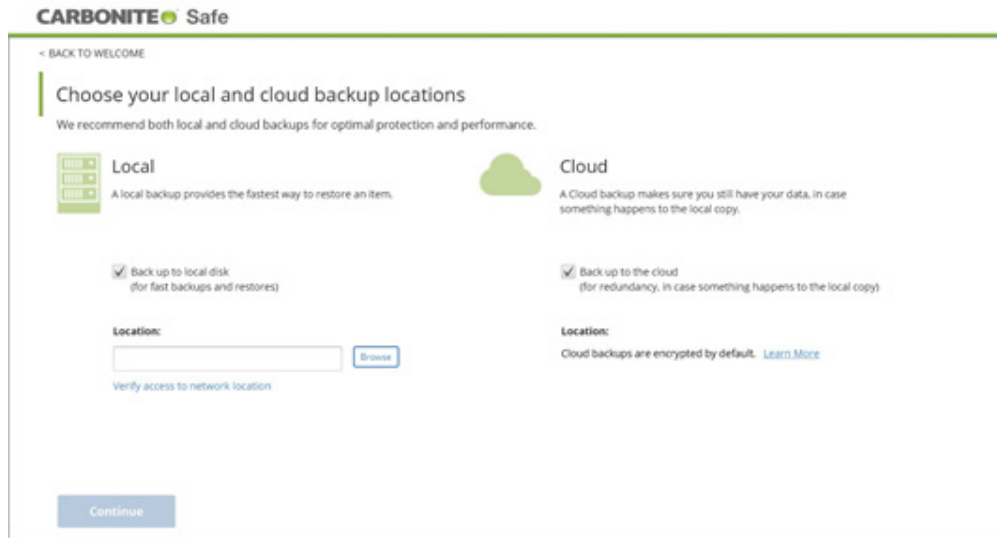
Click **Browse** to navigate to a location on disk where your backups will be stored. Clicking **verify access to network location** will allow you to specify a mapped network drive to be used as your local storage location.

Backing up to disk will allow for faster backups and restores, while backing up to the cloud will create redundancy in case you are unable to restore from a local copy.

After making your selection(s), click **Continue** to proceed.
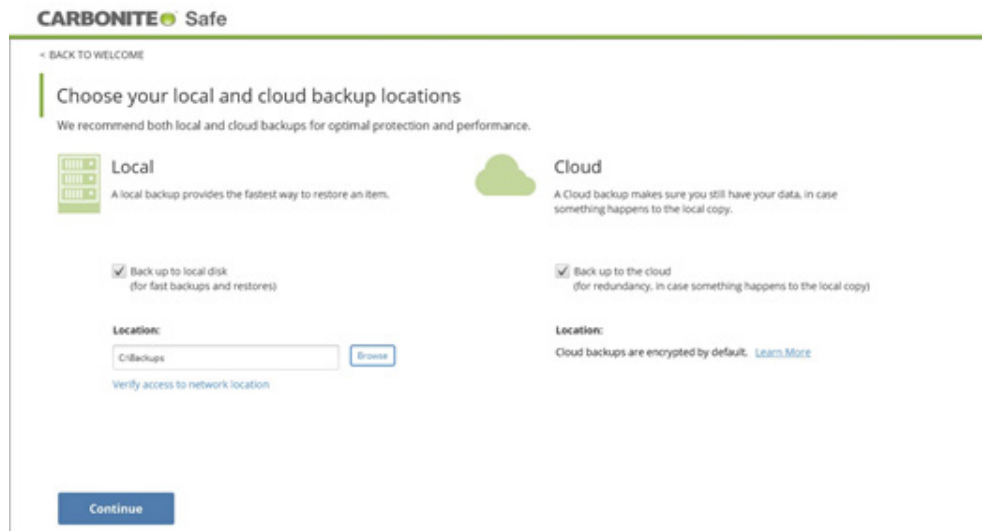
On the next page, you will be able to name your backup set, set a backup schedule, set a retention policy, and select files and folders for backup.

You can also exclude file types from your *File System* backup set. Click the arrow from the drop-down menu for *Exclude Files* to display a list of file extensions.

You can enter a list of file extensions that you want excluded from your backup set such as: ***.pptx , *.docx**. You can also exclude files in a subfolder by entering the path of the folder such as: *C:\Data\[exclude]*, where *[exclude]* is the subfolder that will be excluded from backups.
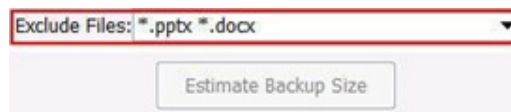
Different backup types will have different options visible throughout the backup set creation process. Not all options you see while creating a File System backup type will appear for other backup types. For additional information about creating a backup set for other backup types, please review this Knowledge Base article.

After making your selections, click **Save & Continue**.
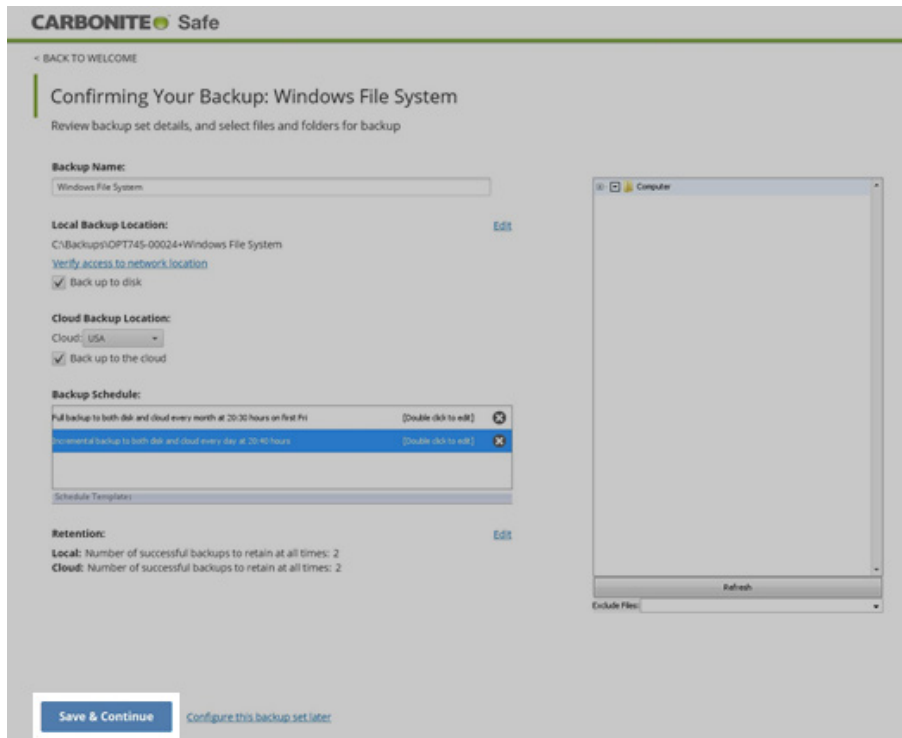
A message will appear once your backup set configuration settings have been registered. Click **Continue** to proceed.
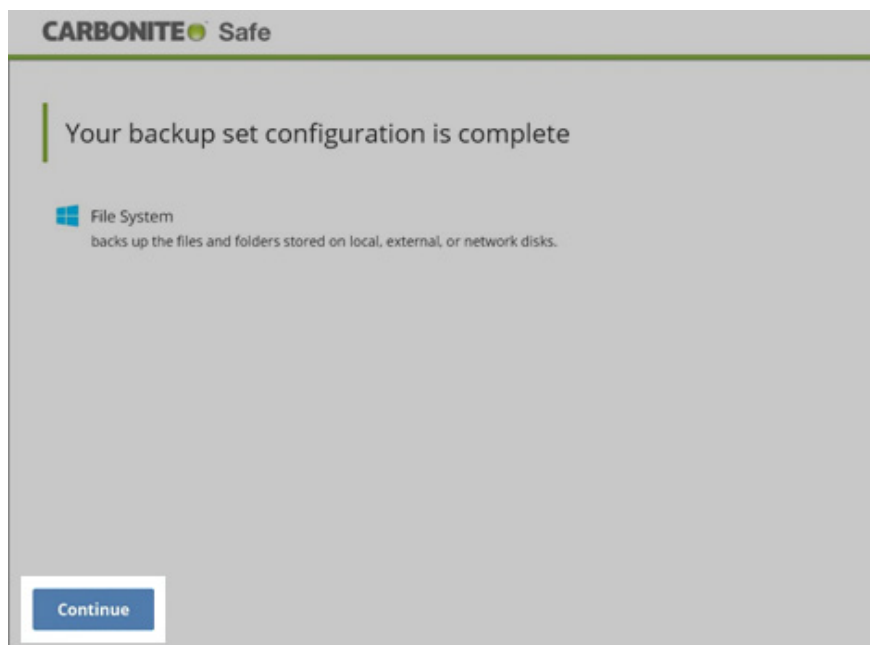
On the next page, a screen will appear advising you to schedule your first full backup run. After setting the date and time, click **OK** to proceed.
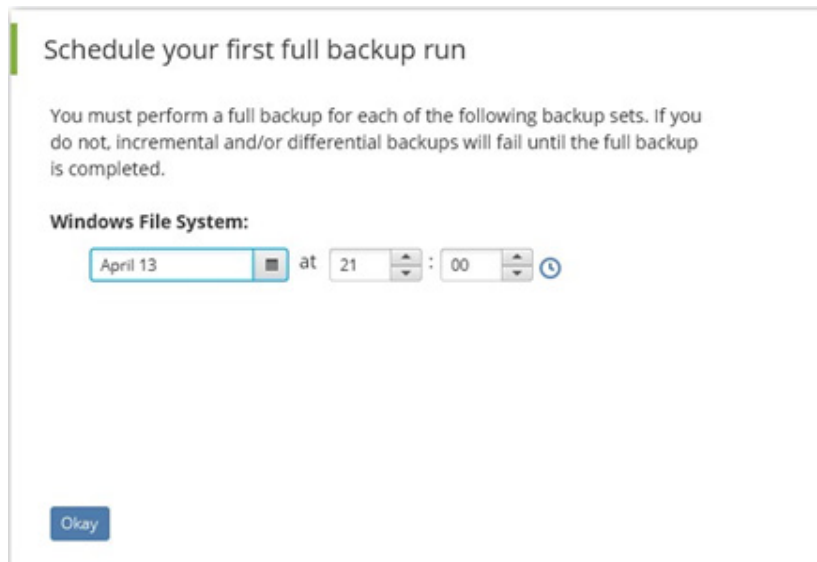
Your backup set configuration is complete. Click **Continue to Dashboard** to proceed.
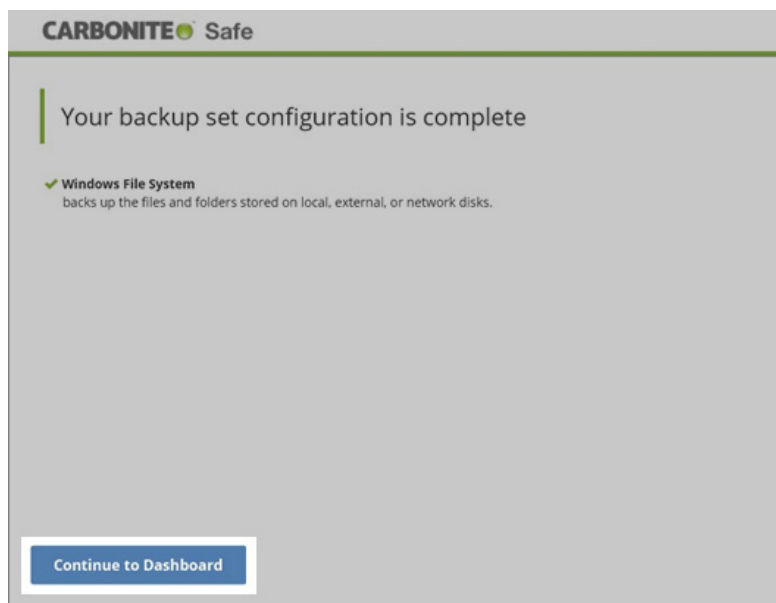
The Dashboard will display information about all your backup sets, such as the backup name and backup type, the total storage used, and other details.
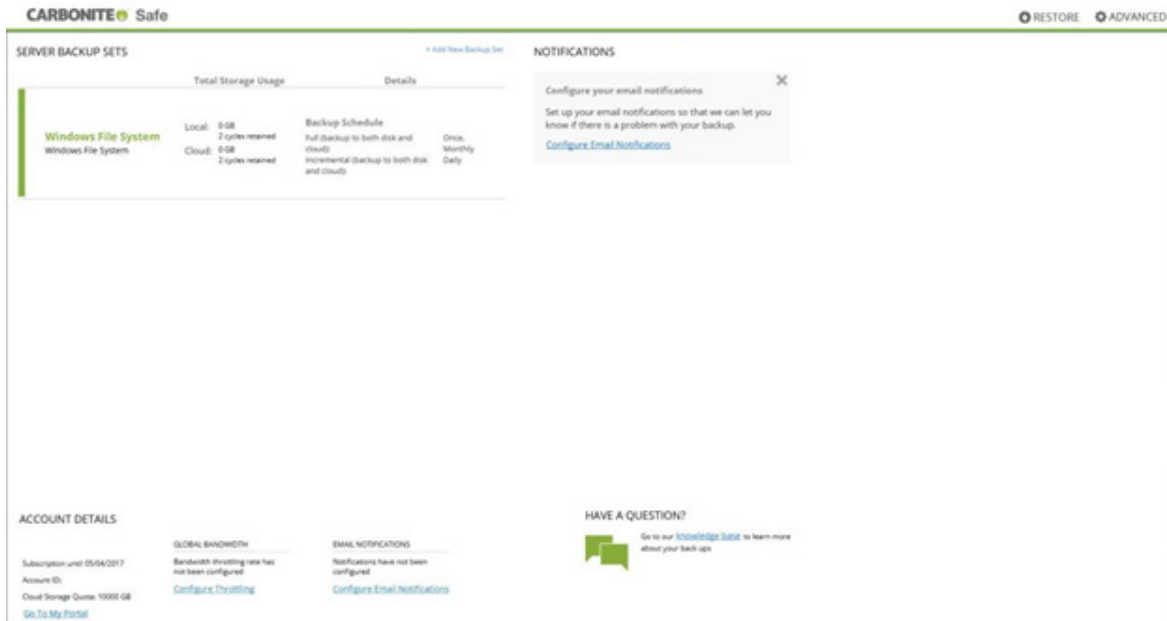
Within the Dashboard, you will also be able to perform the following actions:

- Add a new backup set
- Navigate to the *Restore* page and start a restore.
- Navigate to the Advanced page and <u>import existing backup sets</u>. On that same page, you will also be able to update your *Carboniteuser* password, <u>send log files</u>, <u>connect to an agent</u>, <u>check your version number</u> and perform other tasks.
- <u>Configure your email notifications</u>
- Configure your bandwidth throttling settings
- Access <u>Carbonite's Knowledge Base</u>

Updating Configuration Settings for a Backup Set

CSSB's default backup configuration options represent the minimum settings for backup best practices. Configuring your backup options without following best practices may impact your ability to restore.

> We do not recommend making changes to your default backup configuration settings, unless these changes are necessary to meet your company's backup needs and requirements.

You can opt to update certain configuration settings for your backup set, such as updating your backup location if you are running out of disk space or updating your backup schedule if your current schedule does not meet your backup needs.

After selecting the backup set within the *Dashboard*, click **Edit Backup Set**.

22
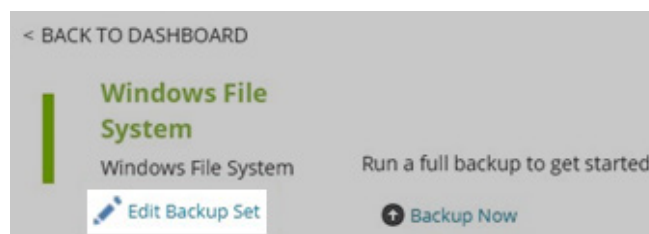
You will be able to make changes to the following options:

- Update your backup location
- Update your backup schedule
- Update your retention settings
- Advanced backup settings such as:
    - Encryption
    - Compression
    - Bandwidth throttling
    - Custom Scripts
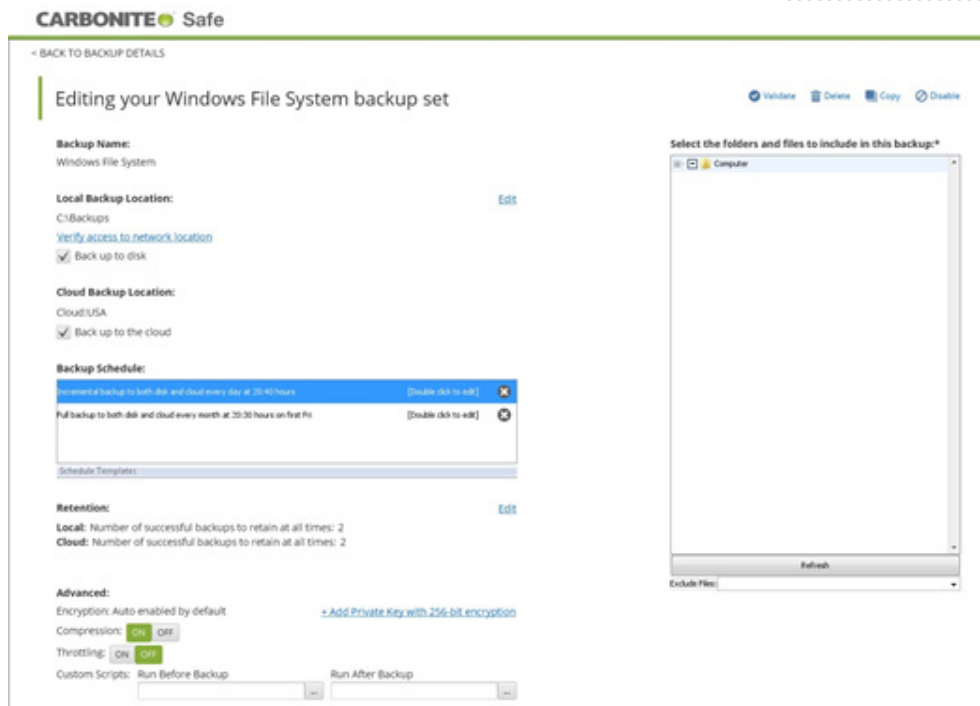
The above screenshot shows the configuration options as it appears for a Windows File System backup set.

On this page, you can also perform the following actions from the available menu options within a backup set:

- Validate a backup set by clicking the link for *Validate*.
- Delete a backup set by clicking the link for *Delete*.
- Copy a backup set by clicking the link for *Copy*.
- Disable and enable a backup set by clicking the link for *Disable* or *Enable*.
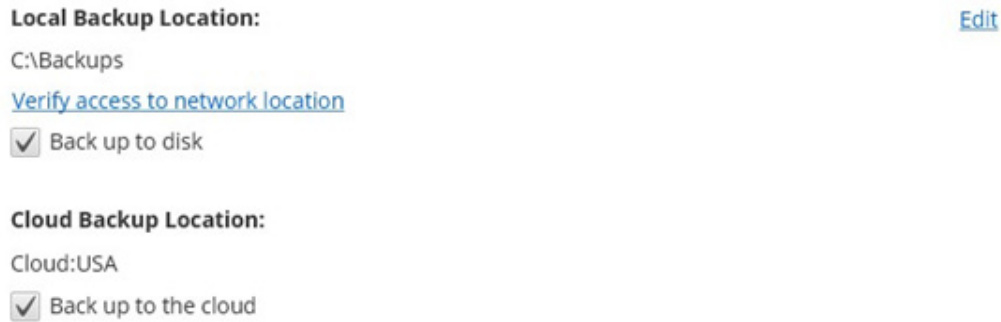
Some options may not be available for all backup sets.

After making your selection(s), follow the on-screen instructions.

For additional information about these menu options, please review this Knowledge Base article.

Update Your Backup Location

Carbonite Safe Server Backup provides the flexibility of backing up to the cloud, to a local disk, or a combination of both.
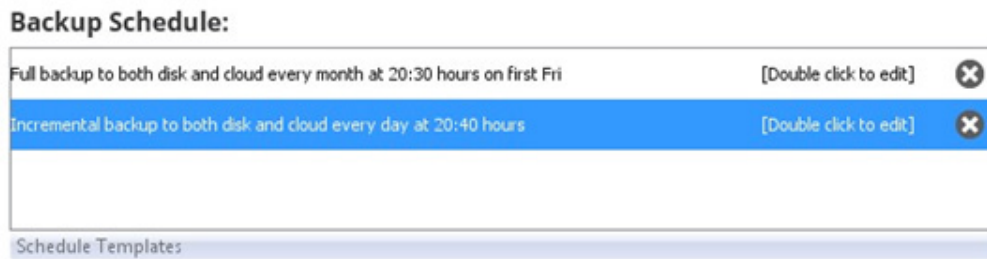
Local Backup Location:

C:\Backups

Verify access to network location

☑ Back up to disk

Cloud Backup Location:

Cloud:USA

☑ Back up to the cloud

Edit

The following options for setting your backup location are available:

- **Local Backup Location:** CSSB supports backing up to a local disk, an external hard disk or a networked mapped drive.
- **Cloud Backup Location:** Carbonite stores your data in secured data centers located across the world. You can choose from the United States and Europe. It is possible to have different cloud storage locations for different backup sets. However, please note that once configured, you cannot change the cloud storage location for a backup set. If data for a single backup set were uploaded to multiple locations, it would be difficult for CSSB to perform restores.

Update Your Backup Schedule

You can add scheduled backup runs for a backup set within the Backup Schedule section.

Backup Schedule:

Full backup to both disk and cloud every month at 20:30 hours on first Fri	[Double click to edit] ⊗
Incremental backup to both disk and cloud every day at 20:40 hours	[Double click to edit] ⊗

Schedule Templates

A backup schedule template can be modified at any time by selecting and double clicking it.

For File System backups, Carbonite Safe Server Backup recommends a monthly full backup and a daily incremental backup. The following predefined templates can be selected when configuring a backup schedule:

24

- **Weekly Full + Daily Incremental:** It indicates a weekly full backup and a daily incremental backup to both the local disk and to the cloud.

- **Monthly Full + Daily Incremental (Recommended):** It indicates a monthly full backup and a daily incremental backup to both the local disk and to the cloud.

- **Monthly Full + Weekly Differential + Daily Incremental:** It indicates a monthly full backup, a weekly differential backup, and a daily incremental backup to both the local disk and to the cloud.

When a new backup set is created, CSSB automatically assigns the recommended *Monthly Full + Daily Incremental* backup schedule to that backup set.

Predefined backup schedule templates will vary for other backup types.

Carbonite allows you to stack different backup types and schedule them according to your preferences. For instance, you can set a full backup to run once a month, a differential backup (backing up everything added to the computer since the last full backup) once per week, and an incremental backup (backing up everything added to the computer since the last incremental, differential, or full backup) once per day.

To stack backup schedules, select the **Add Custom Schedule** option from the *Schedule Templates* drop-down menu.
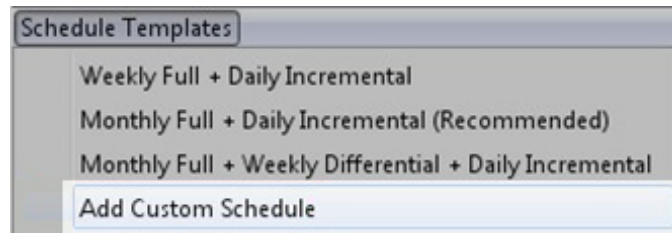
A window will appear with a warning message. Click **OK** to proceed.
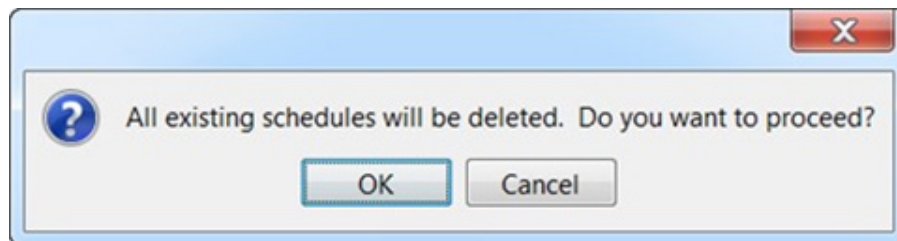
To add a custom schedule, click the **Add Schedule** button to proceed.
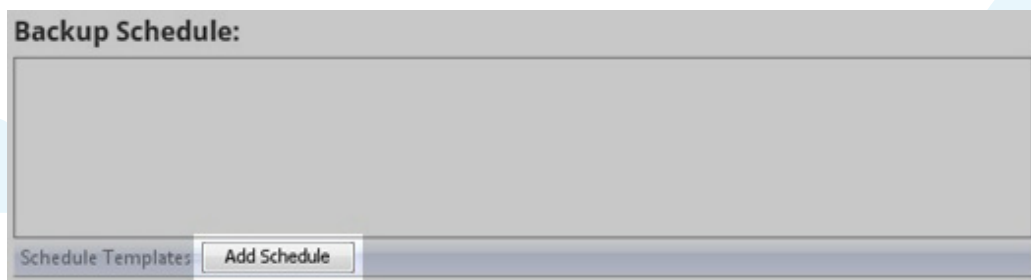
Once a schedule has been added, it will appear in the list of backup schedules.

25

Backup Schedule:

| Full backup to both disk and cloud every day at 22:00 hours | [Double click to edit] | ✕ |

Schedule Templates | Add Schedule
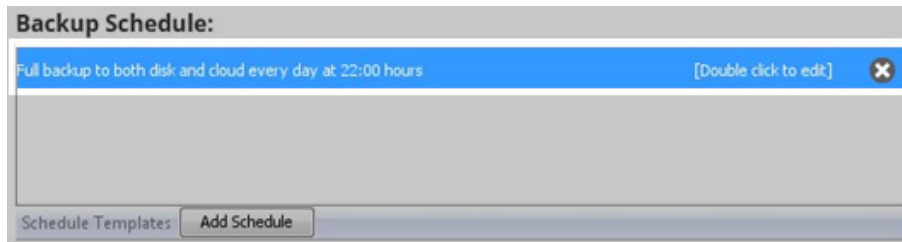
To edit a backup schedule, double click it. A window will appear with customizable options.

Edit Schedule

⦿ Full   ○ Differential   ○ Incremental

Every Day ▾   At ▾   22 ⇕   00 ⇕   Hours

☑ Wake up the system to run the task

OK   Cancel
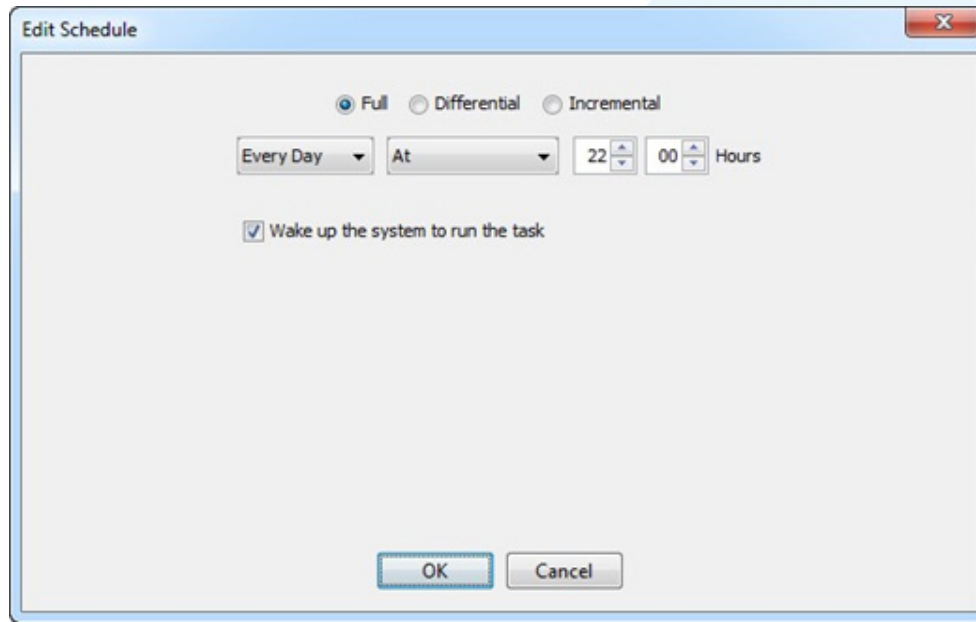
Within this screen, you can run a full, differential, or incremental backup every day, every week, every month or every year at a specific time. You can also specify the following backup options:

- **Full Backup:** This type of backup makes CSSB back up all of the data associated with the backup set.
- **Differential Backup:** This type of backup makes CSSB back up only the data which changed since the last successful full backup.
- **Incremental Backup:** This type of backup makes CSSB back up only the data which changed since the last successful full, differential, or incremental backup.
- **Wake up the system to run the task:** Carbonite Safe Server Backup can also be set to wake the computer to run the backup, if it is in Sleep, Standby, or Hibernate mode. Simply mark this checkbox to enable this feature.

Computers running Windows 7 and Windows 8 operating systems require that you allow wake timers in order for the *Wake up the system to run the task* feature to work properly. Follow the steps below:

1. Click **Start; Control Panel; Power Options**.
2. Locate your currently selected power plan and click the **Change plan settings** link next to it.
3. Click **Change advanced power settings**.
4. Scroll down the list of power settings. Locate and expand the *Sleep* section.
5. Expand the *Allow wake timers* sub-section.
6. Set any appropriate settings to **Enable**.

Update Your Retention Settings

Within the Retention section, you can configure a separate retention policy for backups stored on disk and backups stored in the cloud.

Retention: Edit

Local: Number of successful backups to retain at all times: 2
Cloud: Number of successful backups to retain at all times: 2

Expired backups are purged within 24 hours of expiration.

Backups are only removed by the pre-defined retention policy or by manual deletion. Every backup is added to disk or the cloud without overwriting previous backups, so it is important to set a retention policy that suits your needs while also staying within your chosen storage budget.

While configuring a retention policy, consider the following:

- Importance of older backup data, to ensure that you have access to older files even if those files have been deleted or modified and are not contained in newer backup runs. Past backups also allow for recovery from viruses such as Cryptolocker, which encrypt users' data with unbreakable encryption.

- Free space on disk and/or in the cloud, to ensure that your backups do not fail due to lack of space.

Retention Types

There are two types of retention available after clicking the **Edit** button within the **Retention** section:

- **Number of Cycles:** This option allows users to keep a chosen number of backup cycles. A backup cycle is a full backup plus all associated incremental and differential backups. When a new full backup is completed, excess backup cycles are purged. Please refer to our Knowledge Base article on Number of Successful Full Backups to Retain for more detailed information.

Retention: Stop Editing

Set retention by [Time Retained] [Number of Cycles]
Local: Number of successful backups to retain at all times: 2
Cloud: Number of successful backups to retain at all times: 2

- **Time Retained:** This option allows users to keep backups for a specific period of time. However, a backup will not be purged if another backup depends on it. In other words, no backup in a cycle will be purged until all of the backups in that cycle are ready to be purged. This option ensures that you have all the data that is needed to perform a complete restore to any available backup point, but it does mean that backups can be kept longer than their retention setting suggests.

Retention: Stop Editing

Set retention by [Time Retained] [Number of Cycles]

            Local   Cloud

Full/Differential/Incremental   -1   Retaine... ▼   3   Months ▼

Click **Stop Editing** to register your changes.

27

Retention Values

Carbonite Safe Server Backup offers two special retention values:

- **Forever:** Change the retention value to 0 (zero) to keep backups forever. A backup set to be kept forever will never expire. It will never be purged automatically, but it can be deleted manually. Remember that backups do not overwrite each other. Please ensure that you have ample space on disk and/or in the cloud if you choose to keep backups forever.
- **Retained Until Upload:** Only available for disk backup retention, this causes the backup on disk to be deleted immediately after it is uploaded to the cloud. Only backups that have successfully uploaded will be deleted. Set your retention value to **-1** to use the *Retain until upload* option.

Advanced Backup Settings

Carbonite Safe Server Backup supports compression and encryption of user data. You can manage your bandwidth by specifying maximum upload and download rates to and from the cloud, and advanced users will also be able to run a custom script before or after a backup.

Advanced:

Encryption: Auto enabled by default   + Add Private Key with 256-bit encryption

Compression: [ON] [OFF]

Throttling: [ON] [OFF]

Custom Scripts: Run Before Backup   Run After Backup
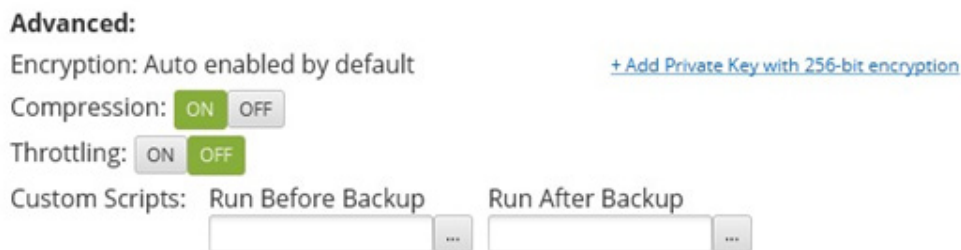
Encryption

Carbonite Safe Server Backup offers two types of encryption:

- **Auto Encryption:** Carbonite Safe Server Backup will automatically encrypt your backups on the cloud using AES 128-bit encryption.
- **Private Key Encryption:** With Private Key Encryption, users create a unique key generated from a passphrase. The encryption key or passphrase is required in order to restore data. Private Key Encryption will encrypt your backups using AES 256-bit encryption. AES 256-bit encryption is trusted worldwide.

Private Key Encryption

With Private Key Encryption, your backups are encrypted using AES 256-bit encryption. The encryption key or passphrase is required in order to restore data.

> If Private Key Encryption is chosen, you are responsible for safe and secure storage of your encryption keys. Carbonite does not store your encryption keys or passphrase anywhere. Replacement keys can be created if you remember your chosen passphrase. If you lose your private encryption key and forget your passphrase, neither you nor Carbonite will be able to decrypt your encrypted backup data.

To create a new private encryption key:

1. Within the Advanced section, click **Add Private Key with 256-bit encryption**.
2. A new window will appear.
3. Enter a *Key Name*. This will be the name of the file stored on disk.
4. Choose a passphrase.

   - The passphrase must be at least four characters in length.

5. Confirm the passphrase.
6. C hoose a location to save your encryption key to.

   - A copy of the key must remain in this location in order to encrypt your backups.

7. Click **OK**. A new window will appear to confirm that the encryption key was created.
8. Click **OK** in the new window.
9. Save the backup set. All future backups for this backup set, local and cloud, will be encrypted using your Private Encryption Key.

   - Past backups, if they exist, are not retroactively encrypted.

To select an existing private encryption key:

1. Within the Advanced section, click **Add Private Key with 256-bit encryption.**
2. A new window will appear and ask you if you wish to use the existing key.
3. Click **Enable**.
4. Save the backup set. All future backups for this backup set, local and cloud, will be encrypted using your Private Encryption Key.

   - Past backups, if they exist, are not retroactively encrypted.

To delete an existing private encryption key:

5. Select any backup set for which Private Key Encryption is enabled.
6. Navigate to the Advanced section of the backup set.
7. Click Delete Private Key.
8. A window will appear to confirm your deletion and warn you that a copy of the key should be kept for decryption purposes.

Existing Private Encryption Keys cannot be modified. To change a key, first delete it and then create a new one.

Auto Encryption

Carbonite Safe Server Backup will automatically encrypt your backups on the cloud using AES 128-bit encryption. Transfer of your backup data to the cloud is secure using the Transport Layer Security (TLS) protocol. The encryption itself takes place server-side on the cloud.

> Auto Encryption only applies to backups stored on the cloud. Local backups will not be encrypted. If encryption of locally-stored backups is required, you must use the Private Key Encryption option.

Compression

Compression makes the backups smaller. A small backup can be uploaded to the cloud much faster than a large one. This can help save network bandwidth and reduce the storage space required for backups. Compression is ON by default, but it can be turned OFF within the Advanced section.

CSSB cannot accurately predict how much any given backup set will compress. Some data, such as text documents and databases, will compress very well. Other data, like most multimedia files, does not compress well.

Bandwidth Throttling

By default, CSSB attempts to transfer data to and from the cloud at the maximum possible speed. Bandwidth throttling allows users to limit the amount of bandwidth used by CSSB. Throttling can be set at a global level (affecting all backup sets), or configured for a specific backup set.

Users may select a maximum bandwidth allotment separately for upload and for download. Also, users may choose to have throttling always apply, or to only apply at certain times. All throttle speeds are in kilobits per second. A value of 0 means the speed is unlimited.

There are two options available for bandwidth throttling:

- **Throttle By Speed:** This option sets a maximum bandwidth allotment that is always on.

- **Throttle By Time:** This option allows you to throttle only at certain times and on certain days. To set time-based throttling, click the buttons for *Max Upload Rates by date and time* or **Max Download Rates by date and time**. A timetable will appear. Select the cells from the timetable shown and input the desired value in the *Maximum Rate (kbps)* box. Click **Apply Custom Rate to Selected Slots** to apply the provided value to the selected slots.

For ease of use, CSSB comes with predefined templates for time-based bandwidth throttling. You can choose a template from the *Choose Predefined Template* dropdown. If you wish to modify the template values, you can select the time slots as described above and configure different values.

Choose Predefined Template ▼
Choose Predefined Template
No throttling
Throttle on weekdays
Gradual throttle on weekdays
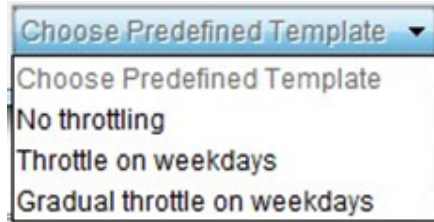
Configured values take effect only for future data transfers. Any ongoing jobs will continue to use any previously configured values

Custom Scripts

CSSB can run batch scripts before and/or after any given backup. There are strict requirements for batch scripts used in this manner. Please refer to our Knowledge Base article on How to Use Batch Scripts with CSSB for more detailed information.

Custom Scripts: Run Before Backup   Run After Backup
[   ] [...]   [   ] [...]

Configuring Email Notifications

CSSB allows users to receive email notifications when an operation completes. Within the Dashboard, click the **Configure Email Notifications** link within the *Notifications* section. Once configured, email notifications are enabled for all backup sets.

NOTIFICATIONS

Configure your email notifications   ✕

Set up your email notifications so that we can let you
know if there is a problem with your backup.

Configure Email Notifications
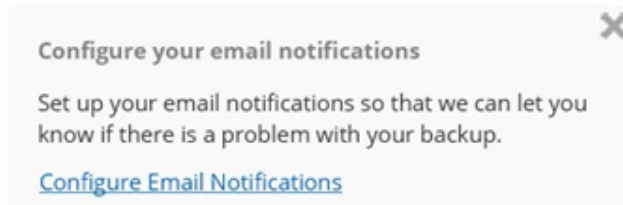
You can also configure email notifications at the bottom of the Dashboard by clicking the **Configure Email Notifications** link.

EMAIL NOTIFICATIONS

Notifications have not been
configured

Configure Email Notifications

By default, emails are sent only when an operation has failed. Emails can also be sent after a success or a warning. Email notifications will not be sent upon success or failure of any restore of the Bare Metal Image backup type. Emails can be sent for all other operations in the Bare Metal Image backup type.

> Emails will not be sent until the SMTP server is configured.

For additional information about configuring email notifications, please review this Knowledge Base article.

Backup Levels

Carbonite Safe Server Backup supports full, differential and incremental backups. Incremental and differential backups are the primary means by which Carbonite Safe Server Backup reduces the size of backup runs after the full backup. Incremental and differential backups are very similar, but have several key differences in how they function.

There are some requirements that must be met for incremental and differential backups to perform their intended functions:

1. Both incremental and differential backups require that a full backup be completed first.
2. You must retain your most recent full backup at all times for a complete restore.
3. Use of incremental and differential backups will create dependencies between backup runs.
4. You can mix incremental backups with differential backups for File Systems backups. Other backup types (such as databases) cannot mix incremental and differential backups.
5. File System backups can be done as incremental backups, differential or both. Backups of other data types, like certain applications may not be supported by incremental and/or differential backups.
6. System State backups can be run as full backups only.
7. No matter what you choose, we recommend you perform a regular full backup.

Full Backup

A full backup will back up all the data associated with a backup set. This type of backup is also referred to as backup level 0. Your first backup should be a full backup. Once it completes, you can use differential or incremental backups to reduce the size of your future backups.

Differential Backup

A differential backup will back up any data that has changed since the last successful full backup. This type of backup is also referred to as backup level 1. Differential backups will start small but grow in size for each subsequent backup, because they contain all changed data since the last full backup. Each one will be larger than the one before it until you perform the next full backup. The rate of growth depends on the amount of data you change. Performing a new full backup will reset the differentials back to their smallest size.

To perform a full restore of all data, you will need the most recent full backup and the most recent differential backup.

Incremental Backup

An incremental backup will back up any data that has changed since the last backup of any type (Full, Differential, or Incremental). This means that all incremental backups will be smaller in size compared to a full backup. This type of backup is also referred to as backup level 2. Unlike differential backups, there is no set growth in file size over time. The exact size of backup depends entirely on how much data changes between backups. A full restore of all data involving incremental backups needs:

1. The most recent full backup.
2. The most recent differential backup, if one was done after the most recent full backup.
3. Every incremental backup that was taken since the most recent full or differential backup.

Backup Set Recommendations

To reap the benefits of both incremental and differential backups, you may combine both types in a single backup set. A backup set that mixes both incremental and differential backups may look like this:

- Do a full backup every month.
- Do differential backups every week.
- Do incremental backups every day.

Back Up to the Cloud

The length of time it takes to back up to the cloud depends entirely on a number of factors. The two most important are:

- Your backup size
- Your upload speed (bandwidth)

For additional information, please review this Knowledge Base article.

Limitations of the Backup to Cloud Operation

Carbonite Safe Server Backup allows users to perform backups to disk only, backups to cloud only, or backups to both disk and cloud. The *Backup to Cloud* operation has a few limitations and drawbacks, when compared to the other backup types. The limitations are technical, and are largely related to the power and speed of the machine that runs CSSB.

The following limitations could affect the *Backup to Cloud* operation:

- The effect of compression and encryption on upload speed
- General stability during large long-running backups
- Recovering from network outages

For additional information about limitations of backing up to the cloud, please review this Knowledge Base article. If your backups to the cloud fail after running for a while, please review this Knowledge Base article.

How to Use a NAS Device with CSSB

Carbonite Safe Server Backup can store your backups on any Network Attached Storage (NAS) device. CSSB can also back up data that exists on a NAS.

Some setup is required. The *amandabackup / CarboniteUser* user created by CSSB during installation must have access to the NAS device. The *amandabackup / CarboniteUser* user is integral to CSSB operations. If the *amandabackup / CarboniteUser* user doesn't have proper permissions to access the NAS, backup and restore operations will fail. Please refer to *What is the amandabackup / CarboniteUser user* for more details.

Five basic steps must be performed before backup or restore involving a NAS device can function:

1. Create the *amandabackup / CarboniteUser* user (or the account specified in Network Location after clicking the *Verify access to network location* link) on the NAS device.

2. Grant the user account permission to one or more folders.

3. Map the shared folder(s) to Windows.

4. Open Carbonite Safe Server Backup and configure your backup set and select your shared folder(s).

5. Start your backups.

For additional information, please review this [Knowledge Base article](#). If you experience any performance issues while running a backup using network drives, refer to this [knowledge base article](#).

Back Up and Restore of Google Drive Data

Carbonite Safe Server Backup can be used to back up and restore data that is synchronized with Google Drive. This allows recovery of the data if it is deleted or if the Google Drive service is unavailable.

For additional information about backing up and restoring Google Drive data, please review this [Knowledge Base article](#).
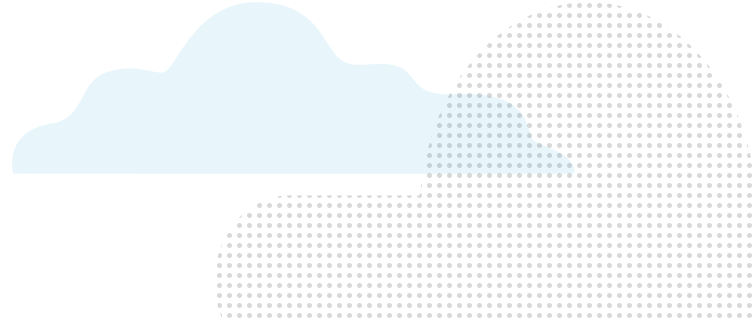
Back Up and Restore of OneDrive Data

Carbonite Safe Server Backup can be used to back up and restore data that is synchronized with Microsoft OneDrive. Both business and personal OneDrive accounts can be protected. This allows recovery of the data if it is deleted or if the OneDrive service is unavailable.

For additional information about backing up and restoring Microsoft OneDrive data, please review this [Knowledge Base article](#).

Back Up and Restore of Dropbox Data

Carbonite Safe Server Backup can be used to back up and restore data that is synchronized with Dropbox. This allows recovery of the data if it is deleted or if the Dropbox service is unavailable.

For additional information about backing up and restoring Dropbox data, please review this [Knowledge Base article](#).
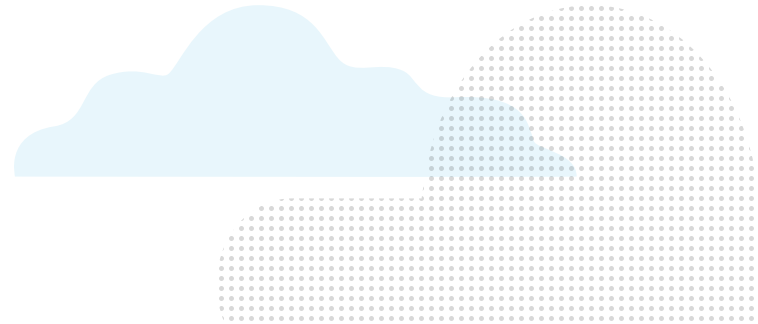
The Backup Details Page

The *Backup Details* page can be accessed by clicking on a backup set within the Dashboard.
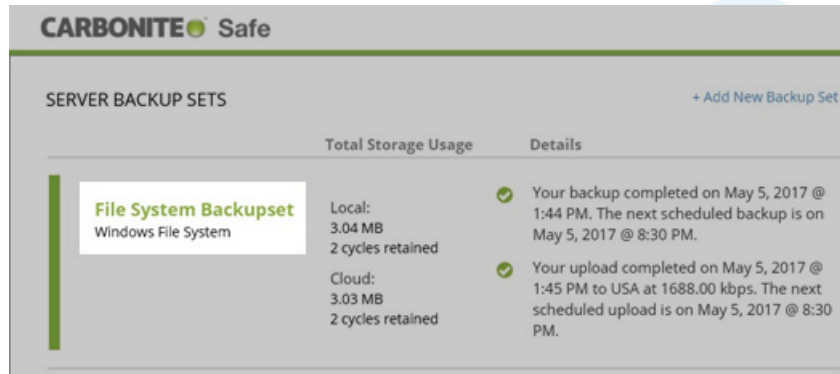
It displays information about your backup status, the amount of data backed up locally and to the cloud, the date and time of your most recent backup, detailed information about your backup runs, and the history of your restore and deleted backup runs.
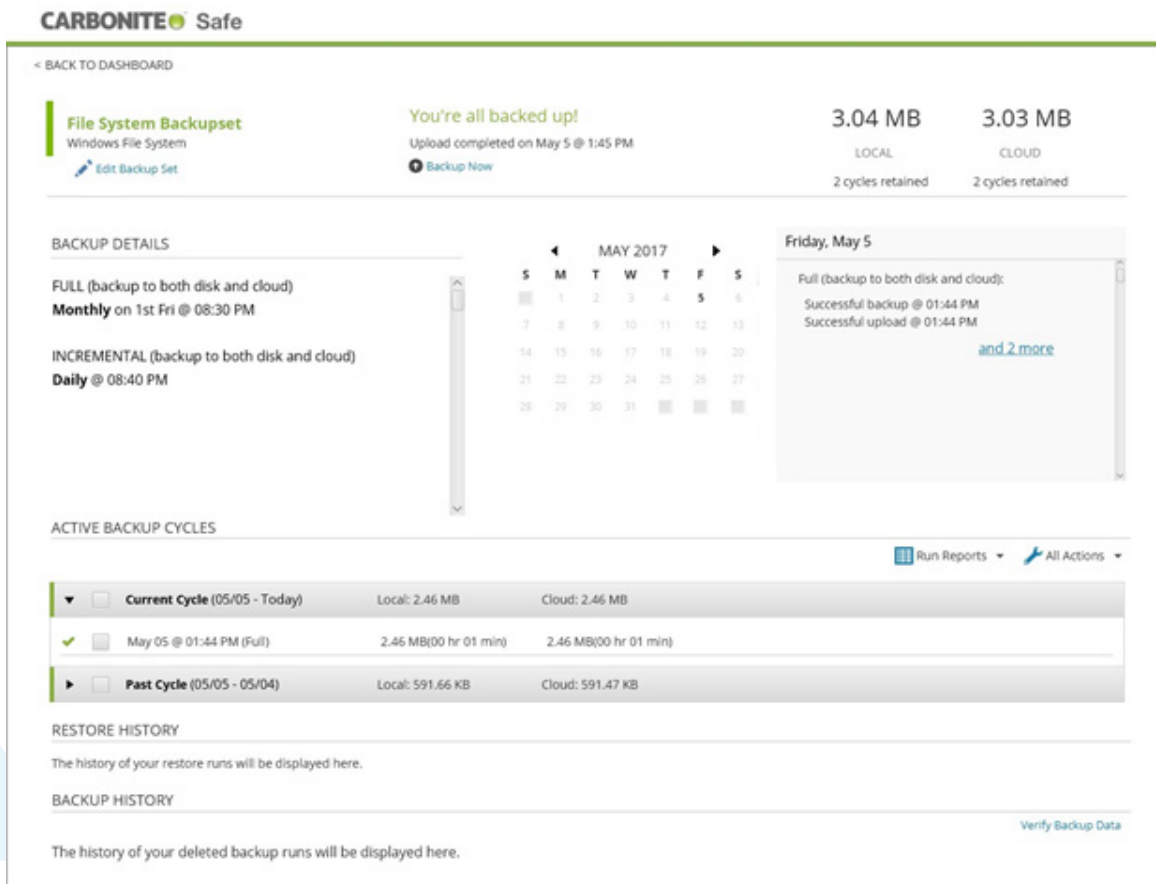
You can perform the following actions on this page:

- *Backup Now* - You can instruct CSSB to perform a full, incremental, or differential backup of any modified data by clicking the Backup Now link. You will have the option of backing up to the following locations:

  - Backup to disk and cloud

  - Backup to disk

  - Back up to cloud

  - Upload backups from disk to cloud

- *Run Reports* - Selecting this option will allow you to run several reports displaying a summary of your backup and/or restore activity. The report(s) will be exported into a Comma Separated Values (CSV) file.
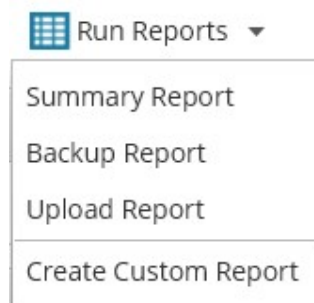
Some of the available reports are as follows:

- *Summary Report* - This report will display a summary of all activity (backup and restore). It will list the backup set name, the elapsed time for all backup runs, the amount of data uploaded, and other relevant information.

- *Backup Report* - This report will display information for all backup operations to the local disk.

- *Upload Report* - This report will display information for all upload operations to the cloud.

- *Create Custom Report* - This option allows you to create a customized report. Follow these steps below:

  1. Within the *Define Report Template* window, specify the template type by selecting the radio button for either *Backup Report* or *Restore Report*.

  2. In the *Template Name* field, type a name for your new template.

  3. Select the columns you want to include in the template view by placing a checkmark in the box next to their name.

  4. Click **Save Template** to add this new template.

  5. This newly created template will appear in the *Run Reports* drop down menu.

- *All Actions* - Selecting this option will allow you to view detailed information about specific backup runs/cycles.

After placing a checkmark next to a backup cycle, the following options will be displayed:

All Actions ▾

Delete Backup Run

View Details

Begin Upload

Pause Upload

Resume Upload

Update Retention Policy

Verify Backup Data
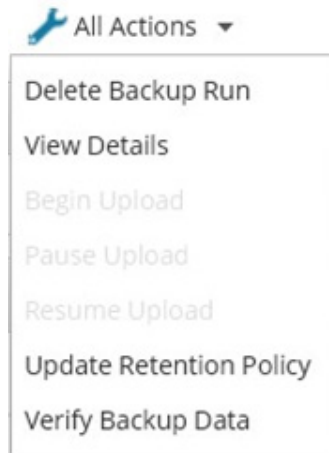
- *Delete Backup Run* - This option will allow you to delete the selected backup cycle locally, in the cloud or both locally and in the cloud.

- *View Details* - This option will display detailed information about the backup run, such as backup host name (server name), backup folder location, whether encryption and compression is enabled, total backup size, cloud location and other pertinent information.

- *Begin Upload* - This option will allow you to upload data from the disk to the cloud. o Pause Upload - This option will be visible if data is being uploaded to the cloud. o Resume Upload - This option will be visible if the upload of data to the cloud was paused.

- *Update Retention Policy* - This option will allow you to change your retention settings for local and cloud backups.

- *Verify Backup Data* - This option will allow you to check the integrity of your backup data.

The *Backup Details* page will also display the following information:

- *Restore History* - A list of all your restore operations will be displayed in this section.
- *Backup History* - A list of all deleted backup runs will be displayed in this section.

The Restore Page

Carbonite Safe Server Backup offers a number of ways to restore file system and application backups. You can restore to the original backed up system or to a different system altogether. When CSSB backs up data, it stores some key metainformation in a special file called the backup catalog. This catalog is used by CSSB at restoration time to let the user select the desired specific data for restoration and to restore the backup data correctly.

You can choose to restore data to the original machine that the data was backed up from or to a different machine.

Restore to the Original Computer

Restoring data to the same computer from where it was backed up is the most common scenario for restoring data. To do this, you must navigate to the Restore page and follow the instructions applicable for the type of backup data you wish to restore. If Carbonite Safe Server Backup is not installed on the original computer, please follow the instructions in the section below to *Restore to a Different Machine*.

Restore to a Different Computer

You can also restore your backed up data originating from one computer to a different computer. This is mostly used to create a clone of the original system. This procedure requires some additional steps before you can launch the actual restore process. There are certain restore requirements that must be met for the type of backup you are restoring.

Note: On the computer you are intending to restore to, it is recommended that you install the same Windows Operating System (with the same service packs) that was installed on the original computer. This is required for restores of System State backups.

Please follow the steps below:

1. Log into your account at https://account.carbonite.com and install Carbonite Safe Server Backup on the target computer (where you wish to restore the backup data).

2. Import the cloud certificate by following the instructions in this Knowledge Base article.

3. Import existing backup sets by following the instructions in this Knowledge Base article.

4. Once the backup sets have been successfully imported by CSSB, you can follow the normal restoration steps applicable to the type of backup you wish to restore.

For additional information about restoring to a different computer, please review this Knowledge Base article.

Restore Encrypted File Systems to a Different Machine

Your backup sets may include files from an encrypted volume or files that are individually encrypted. No special action is required to include these encrypted items in your backups or to restore them to the same computer.

However, if the copy of the Encrypted File System (EFS) private key that is located on the original computer is lost, you will need to use the recovery agent's private key to recover data.

For additional information about restoring an EFS, please review this Knowledge Base article.

Restoring the Windows File System

For Windows File System restores, Carbonite Safe Server Backup gives you a lot of control and flexibility while restoring data. You can restore your files to the original backed up computer or to a different computer.

Important Information about Restoring NTFS Files to ReFS Drives

Some NTFS features are not supported by the ReFS file system. NTFS files and folders can only be restored to ReFS file systems if their properties are compatible.

Files with the following attributes are not supported by ReFS, and therefore will be skipped at the time of restore:

- Named Streams
- Object IDs
- 8.3 Filenames
- NTFS Compression
- Encryption File System (EFS)
- Transaction NTFS
- Hard links
- Extended Attributes
- Disk Quotas

Restore Requirements

The following requirements must be met, whether restoring to the original computer or to an alternate computer:

- The *amandabackup* / *CarboniteUser* user must have full access to the folder where the backups are stored.
    - For cloud backups, this is the chosen Download Folder.
    - For local backups, this is the folder where the backups are stored on the local disk.
        - If the backups are stored in a network location, *amandabackup* / *CarboniteUser* must have access to the network folder. Please refer to How to Use External or Mapped Network Drives with CSSB.
- Likewise, the *amandabackup*/ *CarboniteUser* user must have full access to the folder(s) to which the backups are being restored.

Restoring the Backup Data

To perform a restore of file system data:

1. Navigate to the Restore page and select the backup run associated with the backup set you wish to restore.

2. You will be presented with two restore options:

   - *All items in this backup set* - Choosing this option will restore all items from the selected backup set.

   - *Select items in this backup set* - Choosing this option will allow you to browse or search for items to restore.

3. After making your selection, click **Continue** to proceed.

4. You will be presented with restore settings such as specifying your restore location, and name conflict policy settings.

5. After confirming your settings, click **Continue** to save your changes. Then click **Start My Restore** to start the restore process.

For additional information about restoring a Windows File System, please review this Knowledge Base article.

Restoring other Backup Types

Different backup types will have different options visible throughout the restore process. Not all options you see while restoring a File System backup type will appear for other backup types. For additional information about restoring other backup types, please review one of these Knowledge Base articles:

- Restoring the Windows System State
- Restoring a Microsoft SQL Server
- Restoring a Microsoft Exchange Server Database
- Restoring Microsoft Exchange Local Mailboxes
- Restoring Microsoft Exchange Online hosted for Office 365
- Restoring an Individual Mailbox in Microsoft Exchange
- Restoring Microsoft SharePoint
- Restoring a MySQL Server
- Restoring an Oracle Server
- Restoring Hyper-V
- Restoring a MailStore Archive
- Restoring a Bare Metal Image

Locate Files for Restore

Within the *Restore* page, you can search for a file across all backup runs for a backup set and restore its latest version quickly. This can be useful when you have many backup runs and do not remember which backup run contains the file you need.

For additional information, please review this Knowledge Base article.

Advanced Filtering
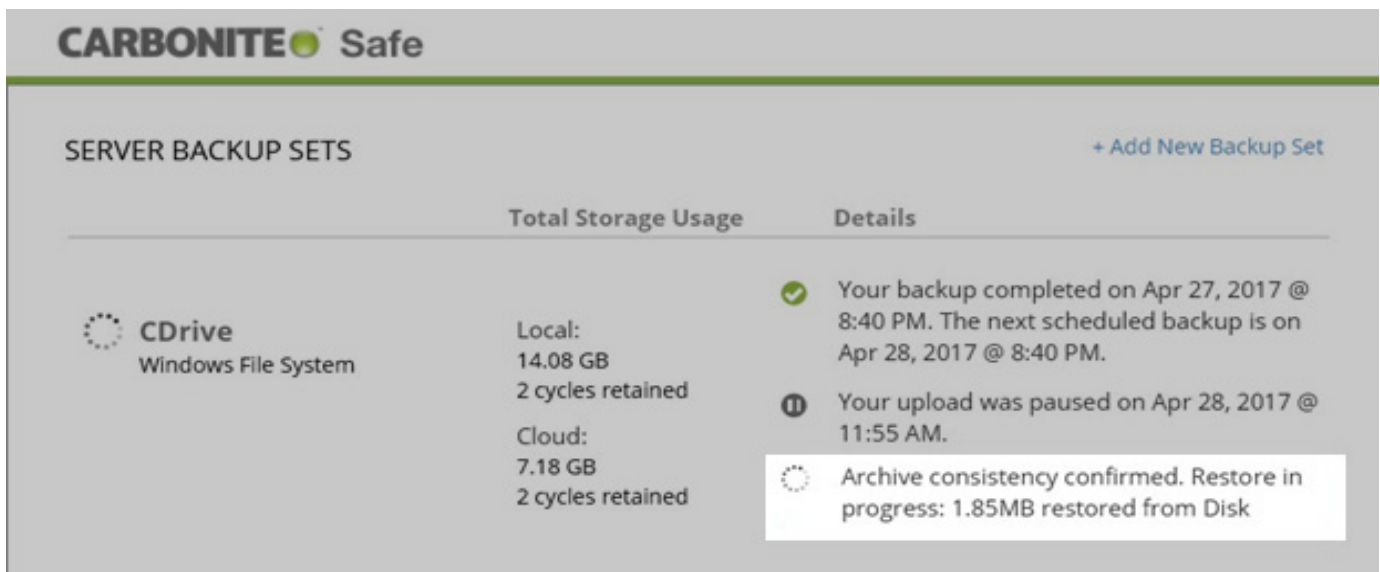
Advanced filtering can be helpful when locating files or folders for restore. This option is available on the *Restore* page of the Carbonite Safe Server Backup Enhanced Interface.

To filter items, users may specify patterns in the Search items input box that include wildcards, combine them with "*and*" or "*or*", as well as apply negation to the whole pattern.

Advanced filtering syntax is used in different locations, depending on which version of Carbonite Safe Server Backup is installed. However, the syntax itself is the same regardless of your version of CSSB. For additional information about advanced filtering, please review this Knowledge Base article.
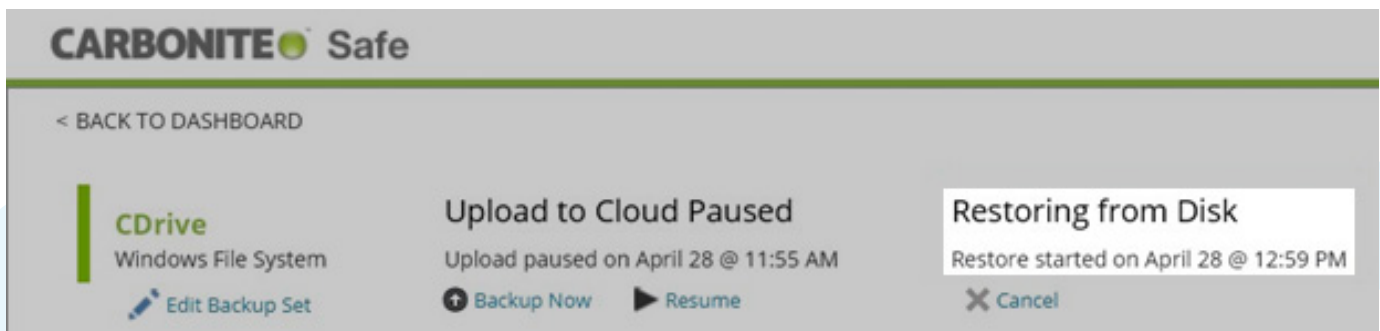
Determine Restore Completion

While Carbonite Safe Server Backup is restoring your data, its progress will be displayed in the *Dashboard*.

The *Backup Details* page, accessible by clicking the backup set being restored, will also display the restore progress. It will list the date and time the restore started.

You can cancel a restore in progress by clicking **Cancel**. For additional information, please review this knowledge base article.

Once the restore has completed, the Details column within the *Dashboard* will display the date and time the restore was completed. It will also display the location of the restored data.

The Advanced Page

The *Advanced* page can be accessed by clicking the **Advanced** link in the upper right hand corner of the *Dashboard.*

The *Advanced* page displays information relating to settings associated with your backup and restore. On that page, you can also view information such as your software version number or get help by remotely connecting to an agent.

Detailed information about these settings is provided below:

Tools:

• **Check Cloud Connection:** This option allows you to verify your cloud connection.

• **Check Dependencies:** This option allows you to verify all dependencies for your backups, by ensuring the correct version of Corretto, Microsoft .NET and PowerShell are installed.

• **Delete all backups finished before [date]:** This option allows you to delete backups finished before a specific date.

• **Enable/Disable Automatic Upgrade:** This option allows you to configure automatic updates for your Carbonite Safe Server Backup software.

• **Import Cloud Certificate:** This option allows you to import your cloud certificate by browsing to its location.

• **Import Existing Backup Sets:** This option allows you to import a local copy of your backup sets or a copy in the cloud.

• **Update carboniteuser Password:** This option allows you to change the carboniteuser password.

About Carbonite Safe Server Backup: Clicking this link will display the version and build number of your software.

Global Settings

- **Data Transfer and Networking:** This option allows you to specify settings for the proxy server used for data transfer to and from the cloud. You will also be able to specify port settings and the number of threads used for downloading and uploading data to the cloud.

- **Global Folders:** This option allows to specify directories used for backups and restores.

- **Retention Policy Enforcement:** This option allows you to set the retention policy for all backups.

Help

- **Change Log Level:** This option allows you to increase the amount of information logged for troubleshooting purposes.

- **Connect to Agent:** This option allows you to remotely connect to an agent while on a support call, to assess any Carbonite-related issues you might be experiencing.

- **Restarting your Background Service:** This option is used as a troubleshooting step for certain Carbonite-related issues.

- **Send Logs:** This option allows Carbonite to collect all necessary log files for troubleshooting purposes. These logs will automatically be uploaded to Carbonite for review.

You can always return to the *Dashboard* by clicking the link for **< BACK TO DASHBOARD** at the top.

Moving Local Backups to a New Folder

It is sometimes necessary to move backups from one location to another on disk. Clicking the **Edit** button for the *Local Backup Location* section will display various options for updating your backup location. This ensures that CSSB can locate, manage, and restore local backups after they have been moved.

If local backups have been moved manually in Windows Explorer, you can also use this function to update the location in CSSB. For additional information about moving local backups from one location to another, please review this [Knowledge Base article](#).

Removing Backup Data with CSSB

As a best practice, one should always set a *Retention Policy* that best suits their business needs. Data that meets its *Retention Policy* is automatically removed from the cloud, providing lower costs and easier quota management. A user can also delete data manually from the cloud using one of the following methods:

• Deleting Backup Run(s) via the *Backup Details* Page

• Changing the Retention Policy for Older Backup Runs

• Deleting All Backup Finished Before a Specific Date

• Deleting Backup set(s) via the Backup Details Page

• Deleting Backup Run(s) via the Online Dashboard

For additional information about removing backup data, please review this Knowledge Base article.

Resolving Common Issues

We have included detailed information about resolving some of the most common issues you might encounter with Carbonite Safe Server Backup. You can always search for self-help articles on our Knowledge Base at https://support.carbonite.com/.

Allowing Access to Microsoft SQL Server

All Carbonite Safe Server Backup operations run as the *amandabackup / CarboniteUser* user. The *amandabackup / CarboniteUser* user must have sufficient access to the Microsoft SQL Server in order to perform backups.

There are two ways to grant access to the *amandabackup / CarboniteUser* user as an SQL server user with the sysadmin role:

- Automatically grant access to Microsoft SQL Server via Carbonite Safe Server Backup
- Granting access via the SQL Management Studio

For additional information, please review this Knowledge Base article.

An Operation Failed Error Message

In certain scenarios, an operation in CSSB may fail with a very simple error message that simply says *<Operation> failed* or The *<Operation> failed unexpectedly*.

The *<Operation>* may be a backup, upload, download, or restore. Examples of error messages include:

- Backup failed
- Upload failed
- Download failed
- Restore failed

These very short, very simple error messages are how CSSB indicates that the operation failed in an unknown or unexpected manner.

The two most common reasons for an *<Operation> failed* error message are:

- The system was rebooted or powered off during the operation
- One or more of CSSB's services or processes crashed

For additional information about this issue, please review this Knowledge Base article.

Backup Failed for Too Many Files

Sometimes, a file cannot be backed up. If too many files are unable to be backed up, Carbonite Safe Server Backup will cancel the entire backup run according to the following rules:

- If the backup contains less than 100 files, the backup will fail if half of the files cannot be backed up.
- If the backup contains 100 files or more, the backup will fail if more than 100 files fail to be backed up.
    - This value can be configured from within the registry:
        1. Locate **HKEY_LOCAL_MACHINE\SOFTWARE\Zmanda\ZWC\1.0\ENGINE**.
        2. Create a new *REG_DWORD* key named **FailedFileCount**.
        3. Use *DECIMAL* values and input any value over 100.

The three most common causes for a file to fail backup are as follows:

- The files are open, locked, or in-use and located on a non-SMB3 network share
- Access to file(s) is denied
- The VSS snapshot could not be created or is deleted during the backup

For additional information about this issue, please review this [Knowledge Base article](#).

Backup Requires an Active Subscription

An active subscription is required to perform new backups to the cloud or to the local disk. If your subscription has expired, all backups will fail with the following error: *Product Subscription has expired. Please renew your subscription or import a valid cloud certificate to continue.*

To resolve this issue and resume backups, you must renew your subscription.

For additional information, please review this [Knowledge Base article](#).

Disk Full Error

Backups require enough free disk space to store the data to be backed up. If you are performing a backup and there is not enough space, the backup will fail with the error message *Disk Full*.

To resolve this error message, perform one or more of the following actions:

- Create more free space
- Choose a different backup location
- Check the type of file system on the backup disk

For additional information about this issue, please review this [Knowledge Base article.](#)

Error: One or more of the VSS writers required for backup have failed

Carbonite Safe Server Backup utilizes a set of built-in Windows functions known as Volume Shadowcopy Services, or VSS, to create snapshots of data for backup.

Most backup types have a specific VSS Writer that is explicitly designed for backup and restore of that specific type of data. For example, there is a SQL Server Writer that is used for backup and restore of Microsoft SQL Server databases.

Some backup types have a single writer, while others have multiple writers. Every writer is controlled by a Windows Service.

The VSS Writers are used by many different applications. Nearly all Windows backup applications, CSSB included, interface with the VSS Writers, as will certain built in Windows features that are not necessarily backups. For example, the System Restore functionality in Windows uses VSS to create restore points so that users can roll back to a known good configuration.

A CSSB backup may fail and report any of the following errors:

- *One or more of the VSS Writers required for backup have failed. Please restart <service>.*
- *One or more of the VSS Writers required for System State have failed. Please reboot the system.*
- *One or more of the VSS Writers required for backup are currently in use by another process.*

This is due to the failure of a VSS writer. If a writer has failed, all operations for all applications that rely on that writer will fail.

It is possible to check the state of all writers on the system using the **vssadmin list writers** command.

For additional information about this issue, please review this Knowledge Base article.

Error: One or more of the VSS Writers required for backup type are missing

Carbonite Safe Server Backup utilizes a Windows feature known as Volume Shadowcopy Services (VSS) to create snapshots of data for backup. Most backup types have a designated VSS Writer that is explicitly dedicated to backup and restore of that specific data type. For example, there is an SQL Server Writer that is used for backup and restore of Microsoft SQL Server databases.

Some backup types have a single writer; others have multiple writers. Every writer is controlled by a Windows Service.

The VSS Writers are used by many different applications. Nearly all Windows backup applications (including CSSB) utilize the VSS Writers, but they aren't used exclusively for backups. For example, the System Restore functionality in Windows uses VSS to create restore points that allow users to roll back to a known good configuration.

Symptoms of This Error

A CSSB backup may fail and report the error, "*One or more of the VSS Writers required for* **<backup type>** *are missing.*"

The **<backup type>** field will populate with the type of backup set for the failed back up. For example, if the error appears when running a System State backup, the error would say *"One or more of the VSS Writers required for System State are missing."*

A list of VSS Writers will be shown after the error message. Internal log files will show the error code:

ZWC_ENG_ERR_NO_WRITER_DATA

For additional information about this issue, please review this [Knowledge Base article](#).

Failed to Restore Files

If you receive a warning that says one or more files could not be restored, the *RestoreErrors.txt* file will list which files failed to restore and the underlying cause for the failure.

One common failure involves shortcut folders. Shortcut folders that were originally located on a mapped drive cannot be restored to a local drive. The error in the RestoreErrors.txt file would appear as follows:

- **5196:3012:24/6/2012:19:55:7:160::Failed to create a file \\?\C:\ProgramData\Carbonite\Carbonite Server Backup\Restore_Folder\amanda (192.168.10.3) - Shortcut.lnk**
- **5196:3012:24/6/2012:19:55:7:160::The file exists.**
- **5196:5256:24/6/2012:19:55:10:252::Failed to restore file \\?\UNC\192.168.10.3\shared\amanda (192.168.10.3) - Shortcut.lnk**

To help resolve this issue, use the information in the *RestoreErrors.txt* to determine the files that could not be restored and the cause.

For additional information about this issue, please review this [Knowledge Base article](#).

How to Install the Java Runtime Environment

Carbonite Safe Server Backup requires the Amazon Corretto 8 to be installed on the system. The CSSB user interface cannot run without the JRE, and backups cannot be configured or managed without the user interface.

The CSSB installation process checks for the appropriate version of the JRE on the system, and prompts the user to install the JRE if it is not detected. The installation cannot proceed until the JRE has been properly installed.

How to Manage VSS Shadowstorage Space

Carbonite Safe Server Backup, like all VSS-based backup applications, requires space for VSS snapshots on any disk which contains data that is part of a backup. This space is known as shadowstorage. Backups will usually fail if there is not enough shadowstorage space for snapshots.

For additional information, please review this [Knowledge Base article](#).

How to Use CSSB to Recover from CryptoLocker and Other Ransomware

CryptoLocker is a virus that essentially holds your files hostage and demands a ransom to get them back. There is no guarantee that paying the ransom will unlock the files. CryptoLocker, its variants, and other ransomware are completely illegitimate. They encrypt your files without your permission, making them inaccessible until they are decrypted. Only CryptoLocker has access to the keys required to decrypt the files it encrypts.

However, CryptoLocker (and other similar ransomware) can easily be defeated with CSSB by restoring the files from a backup taken before the system was infected.

For additional information, please review this [Knowledge Base article](#).

Installation or Upgrade Fails with Error Code 1722

Error 1722 is a generic error that can occur during a new installation of Carbonite Safe Server Backup or when upgrading CSSB from one version to another. This error appears when an unexpected problem occurs and the installation process cannot handle it. It is most frequently the result of a failure to install or start a service or database, but can occur for other reasons. The three most common causes for the error are as follows:

- The amandabackup / CarboniteUser user could not be created.
- The server is under a heavy load, causing the installation processes to time out and fail.
- Interference by security software can block installation of the program itself and/or its services.

> After dismissing the error 1722 warning during an installation or an upgrade, another error code may appear. This second error code can vary, but the most common is error 1603

For additional information about this issue, please review this [Knowledge Base article](#).

Mapped Network Drives Do Not Appear in the CSSB User Interface

If you are running Windows Vista, Windows Server 2008, or a later version of Windows, mapped network drives may not be visible in the CSSB user interface.

This problem occurs because Windows User Access Control (UAC) treats members of the Administrators group as standard users. Mapped network drives, especially those created with logon scripts, may be expecting a different authentication level. This can cause programs to fail to see mapped drives.

A full description of this issue can be found on [Microsoft TechNet.](#)

For additional information about this issue, please review this [Knowledge Base article](#).

Microsoft Database Applications and Multiple Backup Sources

Microsoft produces three database applications: SQL Server, Exchange, and SharePoint. Any given database within any of these database applications should only be backed up by one backup source.

It is safe to back up one database with one source and another database with a different source, but you should take great care if you intend to back up the same database with multiple sources.

Note: In CSSB, multiple backup sources are the most common reasons an incremental or differential backup fails for Exchange, SharePoint, or SQL Server database backup sets. If your full backup was successful, but an incremental and/or differential backup failed, please read this with care. It is very likely that you have a second backup source acting on one or more of the databases selected for backup in CSSB.

For additional information, please review this Knowledge Base article.

One of CSSB's Processes Crash: The Faulting Module is MSVCR*.dll

Most often, one of CSSB's processes crashes when a backup, upload, download, restore, or any other Carbonite Safe Server Backup operation fails, usually with the operation failed unexpectedly error message.

However, this can also be linked to other problems, such as the inability to open the CSSB User Interface or inability to send logs.

Regardless of the overt symptoms, this issue is revealed in full by the Windows Application Event Logs. Within the Windows Application Event Logs, an event indicates that one of CSSB's processes or services has crashed. The event notes that the "faulting module" is *MSVCR*.dll*, where * is a wildcard character.

For additional information about this issue, please review this Knowledge Base article.

Schedules Could not be Added or Modified

The following error appears when trying to add a backup schedule or save a backup set: Schedules could not be added or modified.

This error occurs when CSSB is unable to save changes to one or more backup schedules within a backup set. There are three primary causes:

- Backup schedules cannot be modified if someone clicks **No** on the Windows User Access Control (UAC) prompts that appear when CSSB is launched or schedules are modified.
- This error can occur if CSSB is trying to use a temporary storage directory that is unreachable.
- However, the most common cause is one or more problems with the Windows Task Scheduler. CSSB relies on the Task Scheduler for all schedule-related functions.

For additional information about this issue, please review this Knowledge Base article.

The A: or B: Drives Cannot be Selected for Backup

When configuring a File System backup, the **A:** and **B:** drives do not appear in the file tree, and thus cannot be selected. These drives are reserved by Windows for floppy disks, thus CSSB does not check for the presence of drives on **A:** or **B:**.

To resolve this issue, map your drives to a different drive letter. Once complete, you will be able to include these drives in your backup set.

The Path(s) to One or More Files/Folders Has Changed

When creating a backup set, the user can select any number of files and/or folders. CSSB checks that each of these files/folders still exist as part of the validation process. Every backup must pass validation before the backup will begin.

If a file or folder that was selected has been moved, renamed, deleted, or otherwise changed, then validation of the backup will fail. Moving, renaming, and deleting files and folders is part of the everyday workflow for most users. CSSB now takes that into account and asks for input regarding such files and folders.

A pop-up window will display every file/folder that could not be located and the user is presented with three options:

1. **Do not make changes. I will investigate.**

    - Choose this option if you wish to investigate the missing files/folders.

    - If the missing files/folders are found, simply restore them to their original location.

    - If the file paths were changed deliberately, choose option #2 or #3 below.

2. **Remove these paths from the backup set.**

    - Choose this option to have CSSB remove the listed files/folders from the backup set. This will remove those files/folders from the backup set.

    - A warning will appear if the path(s) change for other files/folders in the future.

3. **Automatically remove missing paths from the backup set configuration.**

    - Choose this option to have CSSB automatically remove all missing paths from all future backups for this backup set.

    - A warning will not appear if the path(s) change for other files/folders in the future. Any and all missing paths will be removed from the backup set without user input.

Troubleshooting Email Notification Setup Issues

Carbonite Safe Server Backup is capable of sending emails after any operation completes with a success, warning, or failure status. CSSB does not have a central email server which sends these notifications. To receive notifications, each user must fill in their own SMTP server information. This can be done by clicking **Configure Email Notifications** within the *Notifications* section.

CSSB email notifications can work with any properly-configured email host, including online email hosts such as Office 365. The SMTP server information provided within CSSB must be correct, and attempts to connect to the server must not be blocked by security settings, firewalls, or other means.

For additional information about this issue, please review this [Knowledge Base article](#).

Collecting Log Files for Troubleshooting

Carbonite Customer Care may request log files from your system if more technical information is required to accurately troubleshoot your issue. In most cases, this can be done from the CSSB Enhanced Interface. Please refer to our Knowledge Base article on [Collecting Log Files for Troubleshooting](#) for more information.

Collecting Log Information if the User Interface Will Not Launch

In certain rare cases, the Carbonite Safe Server Backup Enhanced Interface will not launch. This makes it difficult to troubleshoot issues because most of the support options for the program are contained within the User Interface. In these cases, additional steps must be taken to collect the log files.

The standard CSSB log collection tool can be launched from the Start Menu. Click **Start; All Programs; Carbonite; Carbonite Server Backup; Collect Logs** to launch the log collection tool.

> Don't forget to update the customer care team after the log files have been uploaded. If you do not have a support case, please contact us to open one.

Collecting the Java Stack Trace

In some cases, additional information may be required. The user interface is based on Java, and it is possible to collect a Java stack trace. This information can be used to diagnose the problem that is preventing the Carbonite Safe Server Backup user interface from launching properly. Follow the steps below:

1. [Click this link to download zcbconsole.bat](#).

2. Run this file by double-clicking it.

3. The Carbonite Safe Server Backup UI will attempt to launch.

4. Let it run for a couple of minutes.

5. Open the Windows Task Manager and end the javaw.exe process if it is running.

6. Locate a file named zcbconsole.log in your CSSB Installation Directory.

    • The default CSSB installation directory is *C:\Program Files\Carbonite\Carbonite Server Backup* (for 32bit operating systems) and *C:\Program Files\Carbonite\Carbonite Server Backup(x64)* (for 64-bit operating systems).

7. Send **zcbconsole.log** to the Customer Care Team.

Reinstalling Carbonite Safe Server Backup

You can reinstall Carbonite Safe Server Backup after logging into your account on our website and clicking the *Install Carbonite* button. You should always uninstall the currently installed version of the client. If you reinstall CSSB, you do not have to restart your backup from the beginning again, nor will any backed up data be removed from our servers. Once the installation is complete and you launch Carbonite Safe Server Backup, your existing backup sets should appear within the client.

For step by step instructions on reinstalling, please review this [Knowledge Base article](#).

Configuring Automatic Updates

You can configure Carbonite Safe Server Backup to automatically update when a newer version of the product is available. This will ensure you are always running the latest version of the product.

Within the CSSB Enhanced Interface, click the Advanced link in the upper right-hand corner.


Within the Tools section, click **Enable/Disable Automatic Upgrade**.
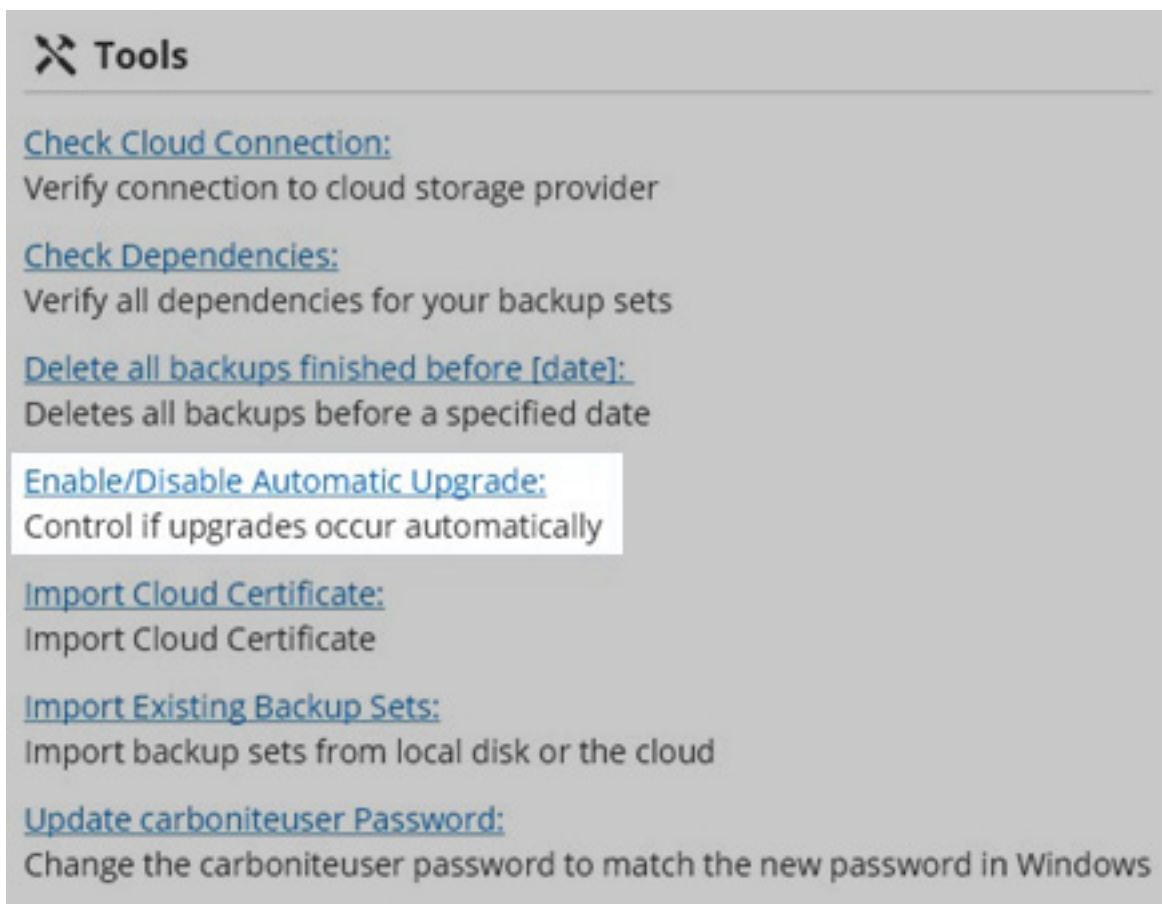
A window will appear, presenting you with two options:

• *Yes, I would like to upgrade automatically* - Selecting this option will automatically upgrade CSSB to a newer version of the product when it is available.

• *No, I will upgrade manually* - Selecting this option will require that you run the installer when a newer version of the product is available.
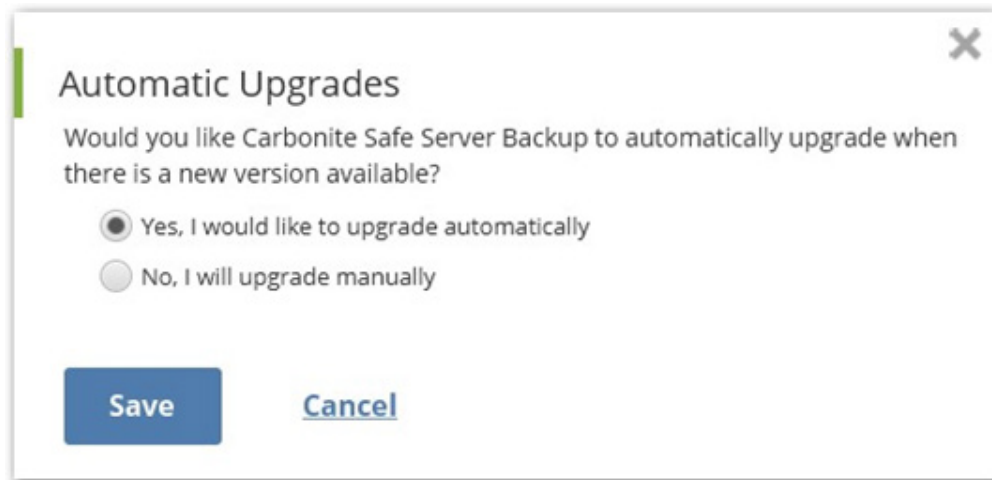
After making your selection, click **Save**.

The Carbonite Knowledge Base

If you have a question about Carbonite that isn't covered in this handbook, our frequently-updated Knowledge Base contains information about every facet of Carbonite.

Carbonite Knowledge Base: https://support.carbonite.com

Searching the Knowledge Base

Our Carbonite Knowledge Base is available for you anytime you need. Simply go to https://support.carbonite.com, input a search term or question, and click **Search**.
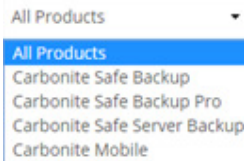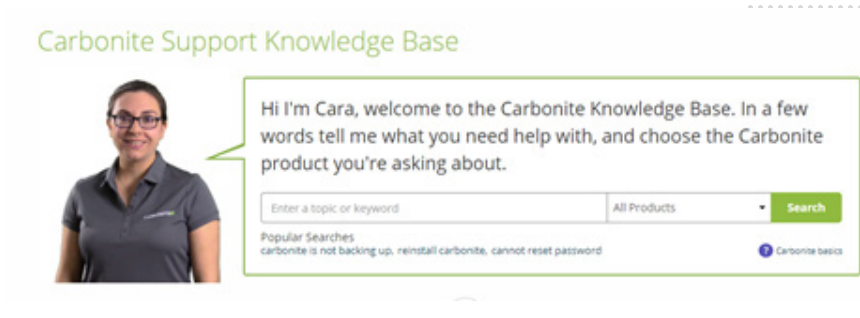
You'll be provided with a list of short articles containing step-by-step instructions that you can follow at your own pace. We recommend using the dropdown filter above the Search Results to select the exact product you have *(see left)*. This will hide any articles that don't apply to the product you're using.