# Installing and Configuring the Backup Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Introduction**

This video shows you how to download, install, and configure the Backup Manager, including scheduling automated backups and initiating your first backup. If you do not know what the Backup Manager is and when it is required, see the related video in this series entitled, *Overview of backup and restore.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Downloading and installing**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Let’s begin by downloading and installing the Backup Manager onto the machine you want to backup.

Do this by following the instructions that were sent to your email inbox in your Welcome letter, or by downloading the Backup Manager client from the https://backup.securewebportal.net web site. If you are downloading the client from the web site, login, and click **Support ->** **Download** on the menu bar. Then select the appropriate version that matches your operating system and architecture. If you have a Windows operating system, you can determine your system information by clicking **Start**, locating and opening the **Control Panel**, and clicking **System**. The operating system version and system architecture are displayed in this window.

After downloading the appropriate Backup Manager client, open the downloaded file to start the install wizard. If your firewall or antivirus program pops up a message, answer the questions appropriately. When the wizard starts, follow each of the prompts to install the client.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Overview of the interface**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now that you have installed the Backup Manager on the machine you want to backup, the next step is to open the Backup Manager and configure it so that you can perform your first backup and start automated backups. Typically, you only need to configure the settings in the Backup Manager once because these settings do not usually need to be changed after they have been configured.

To open the Backup Manager, click the Backup Manager icon on your desktop or in your system tray.

The Backup Manager interface is organized into three main areas: the menu bar across the top, a series of six labeled buttons on the left, and a main information display area on the right. Clicking any of these six buttons displays its associated panel in the main display area. Some of these panels have multiple pages that are accessed by clicking the tabs labels across the top of the panel.

Before we start, let’s preview what’s on each of these six panels.

The **System Status** panel initially has three pages. The first, *Remote Backup Status*, is used to monitor backup activity, manually start a backup, view disk usage, view log files of previous backup and restore sessions, and request technical support. The *Reports* tab is used to view historical graphs and generate reports. The *Software Updates* tab is used to check for software updates and view logs that document the software updates that were downloaded and installed on your system. The **System Status** panel will have up to two additional tabs if you have enabled local server and local disk backups on the **My Account** panel, which we’ll discuss in detail later.

The **Control Panel** display is used to recover or destroy files on the server, access the Web Portal to manage your account, recover a forgotten pass phrase, and view disk usage information for files stored in the cloud. A pass phrase is used to encrypt the data that is stored in the cloud. A pass phrase is different than your account password. We will talk about pass phrases in detail in a later section of this training.

The **My Account** panel is used to configure the destinations where your backup data will be stored, to manage your account, to select data encryption options for locally stored data, and to create and manage your pass phrase.

The **Folders** panel is used to identify or change which data you want to backup. This is done by adding the folders you want to backup, manually excluding selected *subfolders, files, or file patterns* within these parent folders that you don’t want to backup, and creating custom backup policies or rules that further customize which folders and files will be backed up. The Visualize! button on this panel provides an easy way for you to perform these tasks with its color-coded visual display of your folders and files on your system.

The **Schedule** panel is used to set when and how often automatic backups should happen and if they should occur during normal business hours.

The **Options** panels is used to customize other aspects of the Backup Manager, including how you want to be notified when backups start and finish, how many historical versions of the data you want to keep, how the Backup Manager should handle system shutdowns, if you want to constrain bandwidth usage, what your business hours are, and other more advanced configuration tasks.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring My Account**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

With that brief tour of what’s in the Backup Manager, let’s start the configuration task.

To begin configuration, click **My Account** to display the *My Account* panel.

The *Destination for Data* section has preconfigured the *Remote Server* field with the proper hostname of the cloud where your backups will be stored. In addition to backing up your data to our cloud, you can optionally backup data to a server on your private IP network and/or to a local file system accessible by your system, such as a USB drive or NAS device. If you decide to backup data locally, you can also choose whether or not you want that data to be encrypted. Click **Help** on the menu bar to read more about local data backups. Note that data that is backed up to the cloud is *always* encrypted.

We strongly encourage encryption to be turned on for all local backups. If you are backing up sensitive information, such as protected health information, encrypting your backups is required by regulations and must always be enabled.

Next, you need to log in with your username and password. If your password is a temporary password, you will be given the opportunity to change your password. To protect your data from unauthorized access and for billing purposes, you must have an account to backup data to our cloud. If you don't have an account, or have not been given your account user name and password, please contact your sales or support representative.

Enter your account user name and password and click **Test Connection**. This will verify that the Backup Manager can establish a connection to our cloud. This may take a few seconds to verify. A *Connection Verified* message will appear if the connection was successful. If you have problems making this connection, please contact technical support or consult our knowledgebase.

If your password is a temporary password, at this point it will ask if it is okay to change your password. On the change password dialog, enter your temporary password and then enter your new password twice. The rules for passwords are shown in the dialog box. Your password must be at least eight characters long and contain at least one number or punctuation mark. It also cannot contain your account username.

The password strength gauge will automatically display and dynamically update as you enter a new password and can help you gauge the strength of your new password. You should enter a password that results in the password strength gauge reaching into green. Your password should have an estimated strength of at least 24 bits. A strong password will have an estimated strength of more than 32 bits.

Please note that your account *password* is different than your account *pass phrase*. Your account pass phrase is used to encrypt the data that is stored in the cloud. Your account password is used to login to your account in the Backup Manager and in the Web Portal so that you can manage your account. You will create your account pass phrase shortly.

Choosing a strong *password* is very important. If someone can guess your password, they will be able to destroy data associated with your account, and they will be able to access your account information online. They will not, however, be able to *read* the contents of your data unless they also guess your pass phrase.

The Backup Manager will remember your password on your backup computer so that you will not be required to enter it, except when destroying data or changing your password. However, you will need to memorize your password so that you can sign in and manage your account on the Web Portal. If you forget your password, it is possible for your password to be reset.

When you are finished entering your new password, click **OK.**

Next, click **Create Pass Phrase** to create your pass phrase. Your account *pass phrase* is different from your account *password*. Your pass phrase is used to encrypt the data before it is securely transferred over the Internet and stored in the cloud. Choosing your pass phrase is ***the* *most*** important step of the configuration process. Your pass phrase will be used as an encryption key to protect the contents of your data. The security of this encryption depends upon choosing a strong pass phrase. ***You must know your pass phrase exactly as it was entered during configuration to access the contents of your data during a later restore operation.***

To reinforce this point further, the data that is stored in the cloud is unreadable to anyone, including our own staff, and cannot be restored to a human readable format until the exact pass phrase is provided and the data is unencrypted using that pass phrase. The pass phrase that was in place at the time the data was encrypted is the one that must be used in the future to unencrypt the data. The two are inextricably bound together as far as restoring that data is concerned. That is why you would seldom, if ever, change your pass phrase for a given account. If you do change your pass phrase, then you would either have to delete all data in that account and start over, or you would have to remember the old passphrase to unencrypt data from previous backups and the new pass phrase to unencrypt data from future backups.

Although your *account* password can be reset if you forget it, the *pass phrase* cannot be reset under any circumstances. A reset pass phrase would be like using someone else’s key to try to open the door to your house—it simply won’t work, but in this case there are no locksmiths to change the locks either. Remember, y*ou must know the exact pass phrase that was used to encrypt your data to decrypt your data.*

Because your passphrase is so extremely important, the Backup Manager offers the option to save your pass phrase in a dually encrypted form in our cloud. No one will be able to retrieve the saved pass phrase without knowing the exact answers to a number of security questions, which you will create and answer when saving your pass phrase to our cloud. We *strongly* recommend that you take advantage of this option. If you choose *not* to save your pass phrase to our cloud and you forget your pass phrase, you will be *unable* to restore your data under any circumstance. It is *not* possible for anyone to recover your encryption key, *unless* you choose to save your pass phrase to our cloud and can answer your security questions at the time you want to recover your pass phrase. Even if you *do* save your pass phrase to our cloud, if you forget the answers to your security questions, then *no one* can recover your pass phrase, not even Technical Support or anyone else, and you will be *unable* to restore your data.

It is your responsibility to choose a strong pass phrase. If someone can guess your pass phrase, then they will be able to read the data associated with your account if they know or can guess your account password. It is essential to the security of your data that you choose a strong pass phrase. If you are backing up sensitive data, such as protected health information, it is especially crucial that you choose a strong encryption pass phrase.

A strong pass phrase can be generated by using a string of unrelated words, modifying them in unpredictable ways, and inserting random numbers and punctuation. The longer and more random your pass phrase is, the more secure it is. Using a string of familiar words or unmodified words found in a dictionary is lesssecure. You should add or change characters, insert numbers and punctuation, and/or use unpredictable capitalization. Pass phrases must be at least 15 characters long, contain at least two numbers or punctuation marks, cannot contain your username, and cannot contain long sequences of identical or consecutive digits. For more information on generating secure pass phrases, click the link *Is This Secure?* or click **Help** on the menu bar, and search on “pass phrase.”

Create a secure pass phrase and enter and re-enter your pass phrase where indicated. Then click **OK**.

You are now given the option to print your pass phrase. We highly recommend that you print your pass phrase and store it in one or more secure locations.

If you chose to save your pass phrase to the server, the *Security Questions and Answers* dialog box will open. You are required to answer at least three security questions. You will only have to establish your security questions once, so it is better to take the time to choose good questions. When you later try to recover your pass phrase, you will have to answer all security questions correctly in order to recover the pass phrase.

You can select from the predefined security questions, and/or you can create your own security questions. The answers to these questions will be used to protect the pass phrase stored in our cloud and will ensure that only you will be able to recover the pass phrase if it is forgotten. You must remember the exact answers to your security questions to recover your pass phrase or you will be unable to recover your data if you have forgotten or lost your pass phrase. The answers are not case sensitive.

For example, if one of your security questions is “What is the name of the high school you attended?” and you answered “Hillcrest High” when you first answered the security questions but later enter “Hillcrest” when you try to recover your passphrase, the answers won’t match, and you will *not* be able to recover your passphrase. No human will be judging the accuracy or adequacy of the answers to your security questions, so you will have to provide the answers exactly the same as when you entered them here, except for capitalization and whitespace. Punctuation is important, and be sure to use a standard format for any dates you enter that you will later remember.

You also need to enter the name of the person who is answering the security questions so that this person in your organization can be later identified when recovering your pass phrase.

If you choose to store your pass phrase in the cloud as recommended, only a few senior level engineers will be able to initiate the pass phrase recovery process, so it may take some time for the recovery process to be initiated. During the recovery process, you will have to enter the answers to your security questions, not the support staff. This provides an additional level of security that ensures that you and only you will have access to your pass phrase.

After you have selected or created your security questions and entered your answers, click **OK.** Your pass phrase and the answers to your security questions will be doubly encrypted and securely stored in the cloud.

You also have the option of saving your pass phrase on a disk as a plain, unencrypted text file. We recommend that you save the pass phrase to a file and store that file in a different physical location than your backup computer or other safe place, such as on a USB key in a safe deposit box. You might also want to print it out along with your account login credentials and your security questions and answers and store that information in a safe and secure location. The human-readable pass phrase file or printout that you create is like a key to your data so protect it accordingly. You will be asked by the software whether or not you want to save your pass phrase to a file.

If you want to later export your encryption key to a file, click **Store to Disk**, enter your account password, select the location where you want to store the pass phrase file, and click **Save**. The pass phrase file is saved to the selected location. Note that when you export your encryption key using this method, it will only export the binary version of the encryption key and not the plain text version of your pass phrase. The binary version of the encryption key is equally usable for decrypting and restoring your data – the software will accept either form of the pass phrase.

You can also click **Verify** and re-enter your pass phrase at any time to verify that you have remembered the pass phrase correctly.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Selecting files to backup**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The next step in configuring the Backup Manager is to specify the folders that you want to backup.

Click **Folders** to display the *Folders* panel. In selecting folders to backup, please note that selecting a folder also automatically selects all of the folder’s subfolders. The best strategy to follow in identifying the content you want to backup is to first specify which top-level folders should be backed up, and then come back and exclude what you don't need afterwards. For example, if you only want to include a folder *without* including its subfolders, then just add the folder now and use exclusions later to exclude the subfolders.

The Backup Manager automatically excludes certain folders and files on your system by default, such as your web browser’s temporary cache, but you are free to adjust this default exclusion policy if necessary.

There are two ways to add folders to the backup list. The first is to click **Add**, then **Add Folder.**  This opens the *Add Folders* dialog box where you can select a folder from the list on the left and click the green arrow button to add it to the backup list on the right. Click **Save** to save your changes.

The second and preferred way to add folders and files to the backup list is to click **Visualize!** to openthe Visualize window. Visualize! displays your entire system file structure along with check boxes and color coding that indicate which folders and files are currently chosen or excluded in your backup list.

Before we start adding folders to the backup list, let’s see how Visualize! is laid out. Let’s look at the color coding first. The folder or filename with a dark blue background is the one with focus, meaning any actions I take, such as clicking the checkbox or right clicking to bring up the context menu, will apply to that folder or filename. Clicking on another filename or folder name in the list changes the focus to that entry.

Folder and filenames with a light gray background with no checkmark in front of them will *not* be backed up, nor will any of their subfolders. The light gray background also indicates, for parent folders, that you have not manually included or excluded any of the subfolders or files within that parent folder. By default, then, the parent folder and all of its subfolders are not backed up.

Any time you drill down under a folder and begin to include and/or exclude files in the backup list, a light gray checkmark is added in front of the parent folder and the parent folder name is displayed with a dark gray background. If you to “collapse” the parent folder to hide its subfolders, the light gray checkmark and dark gray background tell you that some of the content within that parent folder was selected or excluded for backup. You just can’t see exactly what content was included or excluded because the parent folder is collapsed in the system file list. If you expand the parent folder by clicking the **+** button in front of the folder, you can once again see which folders and files were selected or excluded.

Any file or folder in the system file list with a green background and a dark checkmark in front of its name *will* be backed up, except for any *subfolders* or *files* that you have manually excluded in that folder. The green background and dark checkmark tells you that you initially selected this folder for backup, even if you later manually excluded some of the subfolders and files inside the folder. It tells you that you have consciously decided to include or exclude *each* *and every one* of the files and subfolders under the parent folder.

Note that a parent folder with a green background does *not* mean that this folder and *all* of its subfolders and files will be included for backup. Rather, it means that you initially selected this folder for backup, which did at the time automatically include all of its files and subfolders for backup, but later you might have excluded some of the individual files and subfolders inside that parent folder. Again, a folder with a green background and a dark checkmark in front of its name tells you that you have consciously decided to include or exclude *each* *and every one* of the files and subfolders under that folder.

Folders and file names that have a red background are excluded from the backup list.

So that is how Visualize! color codes the entries in the system file list.

In the columns to the right of these names, Visualize! displays certain information about each entry. For each *folder* in the file list, Visualize! displays how much total data will be backed up for that folder and all of its subfolders and how much data will be excluded from the backup. For each *file* in the list, Visualize! displays the file size and the date the file was last modified. You can drag the borders of these columns left or right to position them for easier reading. When you select or exclude files to be backed up using Visualize!, these columns will not automatically be updated. To update this information after making changes to what you want to be included or excluded from the backup list, right click the mouse anywhere in the Visualize window and select *Refresh Disk Usage* to refresh the information that is displayed.

Visualize! also displays some useful information at the bottom of the screen. The first line displays the full path to the folder or file that currently has focus in the directory structure. The next line indicates two things: whether that folder or file is included in the backup, and the folder policy rules that are attached to it. These rules are created by default by the Backup Manager or when you select or unselect folders for backup or create custom folder policies, which we will discuss shortly.

The next few lines display information on how much data will be backed up. The first line only appears if you have selected a folder that has some content that will be backed up. It displays how many bytes will be included or excluded from the backup for that folder and all of its subfolders.

The next line displays how much data will be backed up on the entire machine across all folders, to help you estimate the amount of total data that will be backed up.

The next several lines display how much data will be backed up for each of the subfolders that contain information to be backed up.

You can refresh the size information at the bottom of the screen to bring it up to date with your changes by right clicking the mouse anywhere in the Visualize! window and selecting *Refresh Disk Usage*. The size information is updated at the bottom on the screen after it has finished scanning your filesystem.

With this overview of the Visualize! window, let’s get back to selecting files for backup.

Our general strategy is to select folders we want to backup and then come back afterwards to exclude specific *subfolders* or *files* from those folders.

The recommended strategy is to add entire top-level folders for backup on the first pass through the hierarchy. You should only add individual *files* to be backed up where you *don't* want to backup most of the data in the folder *and* where you *don't* want to backup any new files that are created in that directory in the future.

With that understanding, let’s start at the top of the hierarchy and add the folders we want to backup.

To do this, start at the highest level of the folder hierarchy and drill down your file structure until you locate a folder that you want to backup. Then click the check box in front of that folder. The folder name appears with a green background, and by default, this folder and all of its subfolders are selected for backup. Don’t worry if you want to exclude some of the files or subfolders underneath the parent folder. We’ll come back and do that in a moment.

Continue doing this until you have selected all of the folders that contain data you want to backup.

The next step is to revisit these folders and exclude any specific files or subfolders that you do *not* want to backup.

To do so, select a parent folder that has a green background, click the **+** button next to the folder name to expand the file list, select a subfolder or filename to be excluded, and remove the check mark in front of that subfolder or filename.

If you unchecked a folder name, that folder name now appears with a red background and all of its files and subfolders will be excluded from the backup.

If you unchecked a filename, the *Create a new filter rule* dialog box appears. Select the desired exclusion option and click **OK**. The filename now appears with a red background.

You can also create custom inclusion or exclusion rules for *folders* that appear with a green or red background. To do this, right-click on the folder name and select *Add include rule* or *Add exclude rule.* Then select *Include custom rule for this folder* or *Exclude custom rule for this folder* and enter a wildcard string of characters that will be used by the rule to determine what to include or exclude from the backup list. For example, if you selected *Exclude custom rule for this folder* and entered *\*smith\**, then any folders in that directory that have the name “smith” anywhere in the folder name would be excluded from the backup list.

You can also right click on *filenames* that appear with a green or red background to create a custom rule for files. For example, to exclude all .exe files from a folder that appears with a green background, right click on any .exe file inside the folder, and select the option *Exclude \*.exe in this folder*. All .exe filenames in this folder will now appear with a red background.

Inclusion and exclusion rules for folders are stored in the folder policy associated with each folder. A Default Policy is also applied. The Default Policy automatically excludes certain folders and files such as temporary files, the recycle bin, Internet caches, Windows system files, and Windows registry files. Advanced users can modify the Default Policy to make system-wide exclusions.

After you make any changes to the Default Policy or to a rule that affects more than a single folder or file, you should *always* use Visualize! to confirm that your change is correct.

You can view a specific file or folder’s applicable policy rules by clicking on the entry in the system file list and viewing the folder’s rules at the bottom of the Visualize! window.

If this seems like a lot to remember, don’t worry. Just try things out. If you don’t like what you did, press **CTRL-Z** one or more times to undo your actions,or right click anywhere on the screen and select *undo*.

When you are completely finished selecting the folders and files you want to backup, click **Save** to save your changes. The Visualize! window closes and the folders and files you have selected for backup are displayed in the *Files and Folders* list of the **Files** panel.

This list displays several things. It displays the folder name that will be used to store the data in each folder. It displays which of the three backup storage locations are currently allowed for backup—to the cloud, a network backup server, and/or a local storage filesystem such as a local USB disk. Note that even though a location is checked here, you must *also* enter in its server name on the **My Account** panel before data will actually be backed up to this location. We recommend that you leave all three of these storage locations checked.  This way, if you choose to implement a second or third storage destination by entering paths to them on the **My Account** panel, the backup will already be enabled.

This list also displays the backup policies that are in effect for each folder, the full path to the folder, and other important notes about that folder.

If you have made changes on the Files panel that you have not yet been saved, click the **Save** button to save your changes before navigating to a different panel.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Scheduling backups**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now that you have selected the files you want to backup, the next step in configuring the Backup Manager is to indicate *when* you want your backups to occur.

Click the **Schedule** button to display the *Schedule: Remote Backup* panel.

To ensure that a recent copy of your data is always available in the cloud, you should schedule *automated* backups. This is done by selecting *Daily* on the *Remote Backup* page and specifying which days you want the backup to occur and what time you want to backup to begin on those days.

If you want more than one backup to occur on each of the selected days, enter how many backups you want per day. The Backup Manager divides 24 hours by the number of backups per day and evenly distributes the backups throughout the day, beginning with the daily starting time. For example, if you enter 2 times per day and a start time of 7 AM, then the backups will occur 12 hours apart at 7 AM and 7 PM on each selected days of the week.

Increasing the number of backups per day ensures that your work is saved throughout the day, but it can also increase the total amount of data stored in historical versions in the cloud. Most users only backup their data once or twice a day.

You can also specify that backups should *not* start during business hours, and you can also specify that a backup should be cancelled if it carries over into business hours. It is very important to note that you should never specify to cancel backups during business hours if you are backing up very large files, such as ShadowProtect image files; instead, you should set bandwidth settings during business hours so that the backups will effectively pause instead. You will indicate what your business hours are shortly in another panel. These first two backup options are particularly relevant if you have limited bandwidth on your network connection and do not want the backups to slow down your business’s network traffic during regular business hours. Another way to control this is by throttling back the bandwidth used during backups, something we will show you shortly.

Finally, if you chose to do multiple backups per day, consider how the choices you make on these first two options will affect whether or not those backups will even occur. For example, if you checked the option to prevent backups from starting during your eight-to-five business hours, and you selected three backups per day with a start time of 7 AM, then the backup that would normally occur at 3 PM will not occur.

Select the next option to wake your computer to backup your data if your computer is in standby mode. Note that this will not turn on your computer if it is completely turned off or has been hibernated.

You should select the next option only if you want to require that you be logged on before a backup can occur. This option is normally never selected except as directed by technical support.

You should always select the final option so that backups will occur within the context of a Windows service and thus can occur regardless of whether any user is logged in or not. If this option is not checked, then the Backup Manager will schedule a Windows Scheduled Task to initiate the backups. Normally this option will always be checked except as directed by technical support.

You can leave the other options on this page as is.

Click **Save** to save your changes before navigating to another tab or panel.

If, in addition to saving your data to the cloud, you are saving data locally and have enabled network server backups and/or local disk backups on the **My Account** panel, additional tabs will be displayed on this panel so that you can schedule those backups as well. These backups can run concurrently, as long as they do not start at exactly the same time. We recommend that they be scheduled at least five minutes apart. Again, before leaving any of these pages, click **Save** to save your changes.

If you are running on a Windows system that requires a password, the *Enter Windows Password* dialog box may appear if you selected an option on this panel that requires it when a backup is started. If it does appear, enter the password associated with your Windows user account. This is *not* your Backup Manager account password. This is the password you use to logon to Windows.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring Options**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The final Backup Manager configuration task is to configure a few more options in the *Options* panel.

Click **Options** to display the *Options* panel. This panel consists of five pages, each of which is accessed by clicking a tab on the top of this panel and using the scroll bar if necessary to see all of the options on the selected page. Clicking on an option displays a brief description of that option on the bottom of the page. You can also adjust the width of the columns on this page by dragging the border left or right to read longer option names.

For most users, the options on these pages can be left to their default setting. However, let’s go through each page and discuss some of the options you might want to review or set.

On the *Notifications* page, you might want to review the default settings for the four *Action* options and change any settings you want. For example, if you don’t want to be notified when your backup starts, click twice on the drop down arrow for that option and select *Do nothing*. Likewise, for the *Action on Finished with Warnings* or *Errors* options, you might want to select *Notify me and send an email with logs*. The email will be sent to the address or addresses specified in the *Email address* option. Normally, you should leave this option on *(auto)* to have the emails sent to the address that was set in the Web Portal.

Typically, all of your notifications are configured using the *Partner Notifications* function in the Web Portal. If your end-user wants to be notified by email of the success or failure of their backups, then you should enable email notifications here on this screen and make sure that the contact email address for their account in the Web Portal includes their email address. If you do rely on the *email* notifications sent by the Backup Manager itself, you may need to adjust the SMTP server settings on this page to facilitate proper email delivery.

All of the other defaults on this page can usually be left as is.

On the *Versioning* page, most partners check the *Limit Number of Versions to Store* option to limit the number of versions that are retained in the cloud and in your local backups, if you are also backing up your data locally. Checking this option helps to reduce the amount of storage space you are using in the cloud. If you don’t select this option and you are using the *Select* service plan for backing up files, each backed up version is kept in the cloud forever, which increases your storage costs incrementally over time. You also might want to check this option if your company is required to keep backups for a certain period of time before they can be deleted for compliance reasons.

There are two ways to limit the number of historical versions stored in the cloud. The first way is to specify the number of days to keep historical versions. For example, enter 365 days if you want all of your historical versions, no matter how many are created, to be kept for a year before they are deleted in the cloud.

The second way to limit the number of historical versions stored in the cloud is to enter the maximum number of versions you want to keep. For example, enter 10 if you want the current version and the last 9 historical versions to be kept in the cloud. Historical versions beyond that number will be discarded. Entering *-1* in this field means “infinity” or “keep every version.”

If you specify *both* a maximum number of versions and a retention period, then whatever limit is reached first is used. The more restrictive value takes precedence. Versions beyond the first limit reached will no longer be retained in the cloud, except as constrained by the *Minimum Number of Versions to Keep,* which we will discuss next.

Set the *Minimum* *Number of Versions to Keep* option to the number of versions of backups you want to keep as a *minimum* before the backup engine is allowed to destroy versions. For example, if you specify three versions to keep, then three backed up versions of each file will always be kept in the cloud—the most recent version plus the two most recent historical versions—even if these historical versions are older than the number of days you specified in the *Number of Days to Keep Historical Versions*. In this example, this would ensure that you will always have at least three backups of every file stored in the cloud.

With regard to historical version limits, keep in mind that when a scheduled backup begins, the Backup Manager sends a new historical version to the cloud *only* if the data being backed up has changed since your last backup. For example, if you limit the number of versions to keep to three, even though you are backing up your data daily, if a file only changes once a week, then the oldest version of the three historical versions would be three weeks old, not three days.

The *Number of Days to Keep Deleted Files* option has to do with files you delete on your local machine. The next time a backup occurs, if the deleted files have previously been backed up, then they will be marked as deleted in the data stored in the cloud and in your local backups, if you are backing up data locally. Deleted files can be restored for as long as you specify in this field. Note that the *Basic* service plan does *not* limit how long you can keep deleted files.

You should set the *Number of Days to Keep Deleted Files* to be equal to what you entered in the *Number of Days to Keep Historical Versions* option to avoid risking incomplete historical snapshots. For example, if you set this option to 30 days and the *Number of Days to Keep Historical Versions* option to 365 days, you would be unable to recover a file you deleted on your local system after 30 days, even though historical versions of files are being kept for 365 days. This is because deleted files are removed from the backed up data across all of the historical backups when the time limit for keeping deleted files has been reached.

The *Destroy Excluded Files* option has to do with changes you make to your backup policy in the Backup Manager. For example, suppose you have been backing up for the last year and you no longer need to backup one of the directories that is included in your backup list, but you don’t want to delete that directory from your local computer. This option is asking if you want to destroy the data that has previously been backed up but is now excluded from the backup policy. Checking this checkbox is the same as answering “yes” to this question. These files will then be deleted from the cloud and your local backups during the next backup session. But the excluded files will still be retained on your local machine.

The *Destroy Deleted Files* option determines how frequently backup sessions will check for old deleted data that should be purged according to the *Number of Days to Keep Deleted Files* option. Checking for deleted files requires additional communication with the cloud for each folder that has been backed up, and for a backup that includes many folders this can cause the backup to take longer than normal. Thus, this operation is normally only performed once per week.

On the *Backup* page, the default settings should work for most users. If you are directly backing up Exchange information stores, then you should enable the *Restrict Concurrent Backups* option on this page. If you have trouble with Microsoft VSS reliably taking snapshots of the data being backed up, technical support may have you adjust some of the settings in this section.

On the *Bandwidth* page, specify your business hours. This information is used by the bandwidth settings, as well as the options *Do not start backup during business hours* and *Cancel backup if still running during business hours* that are foundon the *Schedule* panel.

The options in the *Bandwidth Usage* section of the *Bandwidth* page should be customized to match how much Internet bandwidth you want backups to use during business hours and during off hours. This will allow you to throttle back the Internet bandwidth used by backups so that more bandwidth is available for other applications. Backups will take longer when they have been throttled back due to the self-imposed reduced bandwidth restrictions.

On the *Advanced* page, review the settings in the *Software Updates* section. *Check for New Versions* indicates how often you want the Backup Manager to check for new versions of itself. This option is normally set to *Daily*.

*Automatically Install Updates* indicates whether updates to the Backup Manager should be automatically installed after they are downloaded. Do not use this option if you are using a software firewall that requires your permission when new programs try to access the Internet.

If the *Treat Minor Versions as Major* option is checked, then minor software updates that include reliability fixes but not feature enhancements will also automatically be installed, as long as the *Automatically Install Updates* option is also checked.

The *Software Security* options allow you to deny any configuration changes in the Backup Manager unless the user is able to verify the account password. This will prevent unauthorized configuration changes to the backup policy, allowing you to enforce any change management policy requirements your organization may have.

The rest of the options on this page are advanced options that normally are left to their default values.

After you have completed making all of your selections on the *Options* pages, click **Save** at the bottom of the screen. This button will be grayed out until you have made changes to one or more of the options on these pages.

Congratulations! You have now configured the Backup Manager and are ready to perform an initial backup, which, depending on the amount of data to be backed up, may take a long time. After the initial backup has finished, future backups will be much quicker.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing an initial backup**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If you have a large amount of data—say, more than 50 GB—we recommend that you use a USB preload to do your initial backup. This involves using the Backup Manager to encrypt and backup your data the first time to a locally connected USB drive, and then physically sending your drive to the service center, where our service engineers will load the data into your cloud backup account and take your account out of maintenance mode so your normally scheduled backups can continue. No other backups should occur during this period. After you have generated preload data, do not take the account out of maintenance mode. Contact technical support or consult our Knowledgebase to learn how to perform a USB preload.

To see how much data you have selected for backup, click **Folders**, then **Visualize!.** The total amount of data that will be backed up is displayed at the bottom of the *Visualize!* window.

If the amount of data to backup is less than 50 gigabytes, or if you have a fast Internet connection and want to upload the initial data to the cloud over the Internet, click **System Status** to display the *System Status* panel, click the **Remote Backup Status** tab if that page is not already displayed, then click **Backup Now**. The Backup Manager will immediately begin backing up your data, and a log file recording its progress is created. You can monitor the status of your backup in the upper part of the page. You can also double click on the log file in the lower part of the page.

If your backup is interrupted abruptly because your system temporarily goes down or is manually shut down, the Backup Manager will resume where it left off the next time your system is booted up and functioning again. You can also manually interrupt or cancel a backup at any time by clicking **Interrupt** on the *Remote Backup Status* page of the *System Status* panel and selecting *Pause* or *Cancel*. You can manually resume a paused backup by clicking **Interrupt** again and selecting *Resume Backup*. These options might be helpful if, during a backup, you need to temporarily pause a backup to upload a large business file over the network using the full available bandwidth of your network connection.

You can hide the Backup Manager by clicking the “x” in the upper right corner of the window. You can show the Backup Manager again by clicking on the Backup Manager icon in the windows tray, or by starting the program using the start menu. Note that the Backup Manager will continue running while it is hidden. If you need to completely exit the Backup Manager, go to the *File* menu and choose *Exit.* Note that scheduled backups will continue to start even if the Backup Manager is not running.

Even when the Backup Manager has been hidden or closed, if a backup is in progress, it continues to run in the background. You can monitor the progress of your backup at any time by clicking the Backup Manager icon on your desktop or in the system tray to open the Backup Manager, clicking **System Status** if that panel has not already been selected, and clicking the **Remote Backup Status** tab, if that page is not already displayed. The live status of the backup is displayed on the upper part of the page.

After your backup has finished, double click the log file on the *Remote Backup Status* page of the *System Status* panel to open the log viewer. Use the menu bar at the top of the viewer or press **F1** to display a list of navigation keys you can use to inspect the log file for any errors and warnings. Our knowledgebase has information on the most common errors and their causes. If you need assistance troubleshooting any errors or warnings, please contact technical support, and we’ll be happy to assist you.

You have now successfully configured your backups, performed your initial backup, and started your regularly scheduled automated backups.

If your local system ever completely crashes and cannot be repaired, you will need to install the Backup Manager on a new system. To do so, since you have already established and configured a backup account, you need to follow a different procedure from the one for first-time users that we have been discussing in this training. Instead, download the Backup Manager from the Web Portal as you did previously, click the **Backup Manager** icon on your desktop or system tray to start the Backup Manager, click **Help**, search on the phrase “Restoring after a system crash,” and follow the instructions that are presented there.

If you have further questions on any of the options or functions of the Backup Manager, please click **Help** from the menu bar and select *Contents* to open up the Help database. Here, you can review the *Getting Started* guide, get detailed instructions on other features of the Backup Manager, such as network server backups, see the *Backup Manager Quick Reference*, read how to restore data in the *File Manager Quick Reference*, read about the *Disk Usage Inspector*, see the *Email Archiving Quick Reference*, and review *Frequently Asked Questions*. You can also click the **Index** or **Search** at the top of the help window to use these functions to help you find information. Note that with Index or Search, you must *double* click on an entry on the left side of the window to display the information for that entry. If you cannot find the answer to your question from any of these resources, please contact technical support.

Thanks for watching this tour of the Backup Manager. Please see the other overview and how-to videos in this series for additional training on partner-related tasks.