



# BDR for ShadowProtect Solution Guide and Best Practices

Updated September 2015



## Table of Contents

|   |    |
|---|----|
| Process Overview .....                                | 3  |
| 1. Assess backup requirements.....                    | 4  |
| 2. Provision accounts.....                            | 4  |
| 3. Install ShadowProtect.....                         | 5  |
| 4. Prepare to configure ShadowProtect .....           | 5  |
| 5. Configure ShadowProtect .....                      | 5  |
| Add additional managed computers to this console..... | 6  |
| Connect and manage from this console .....            | 6  |
| Activate a license.....                               | 7  |
| Create a new destination.....                         | 7  |
| Create a new backup job.....                          | 8  |
| Configuring ImageManager .....                        | 11 |
| Customizing retention settings .....                  | 13 |
| Configuring eFolder Online Backup Manager.....        | 14 |
| Create a preload (seed) drive.....                    | 20 |
| Restoring, migrating, or virtualizing servers.....    | 20 |
| Restoring individual files.....                       | 20 |
| Recovering from a disaster .....                      | 21 |
| Additional assistance .....                           | 21 |

## Process Overview

This Solution Guide will walk you step-by-step through the process of implementing your customer's **StorageCraft ShadowProtect** software with **eFolder BDR for ShadowProtect's** services.

To complete this process for your customer, you will:

1. Assess the backup requirements of your customer.
2. Provision eFolder accounts for computers that will be backing up data remotely.
3. Install ShadowProtect on those computers requiring volume-level backups.
4. Prepare and then configure ShadowProtect to perform volume backups of OS and critical server applications.
5. Configure eFolder Online Backup Manager to backup other files and your ShadowProtect volume backup images.

This Solution Guide will also briefly discuss how to

- Add managed computers to the ShadowProtect console,
- Connect and manage computers once they are on the ShadowProtect console,
- Activate a license,
- Create a new backup job,
- Configure ShadowProtect ImageManager,
- Restore, migrate, or virtualize servers,
- Restore individual files, and
- Recover from a disaster

If you have questions, wish to deviate from these guidelines, or have a different version of ShadowProtect, please contact us first at [support@efolder.net](mailto:support@efolder.net).

## 1. Assess backup requirements

Assess the backup requirements of your customer by identifying the following:

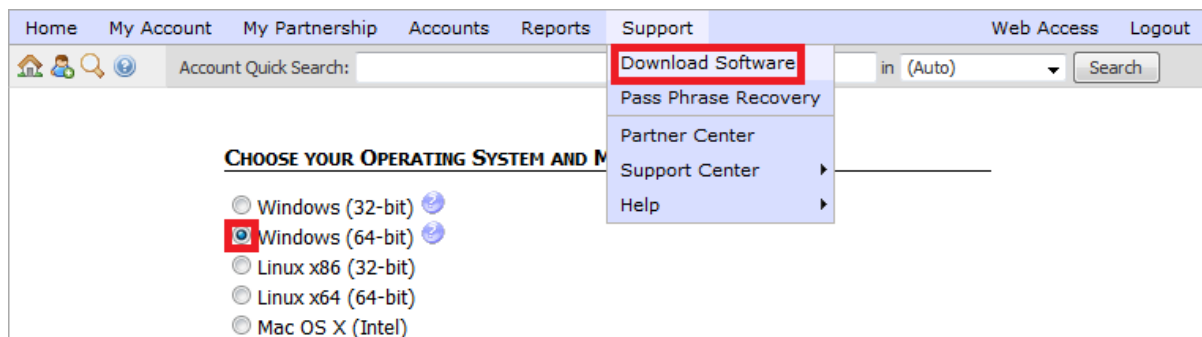
- Critical application servers, such as Exchange, SQL, and SharePoint
- The recovery point objective for critical applications
- Where to store volume backup images
- Data that must be retained for years, because of compliance or company policy
- Files that users may want to restore individually or access from the web

## 2. Provision accounts

- a) Create an account as needed on the **eFolder Web Portal**.  
For complete instructions, see [Create an account using the New Account Wizard](#).
- b) Verify that the correct versions of **ShadowProtect** and **ImageManager** are installed.  
The *Download Product Installers* link is available in the top left corner of <https://msp.storagecraft.com/msp/>



- c) Download **eFolder Online Backup Manager**, if needed, by hovering over **Support** on the eFolder Web Portal and selecting **Download Software**. Select the desired version. Scroll to the bottom of the page, click the **Export Regulation Compliance** box to agree, and then click **Download**.



### 3. Install ShadowProtect

Install ShadowProtect on each server that requires volume backups.

**Do *not* use the PUSH install included with ShadowProtect.** Instead, use the installable package and install the **complete** package on your agents being backed up.

**Note:** The server must be rebooted prior to performing the first full backup.

### 4. Prepare to configure ShadowProtect

Prior to configuring ShadowProtect, complete the following preparation steps:

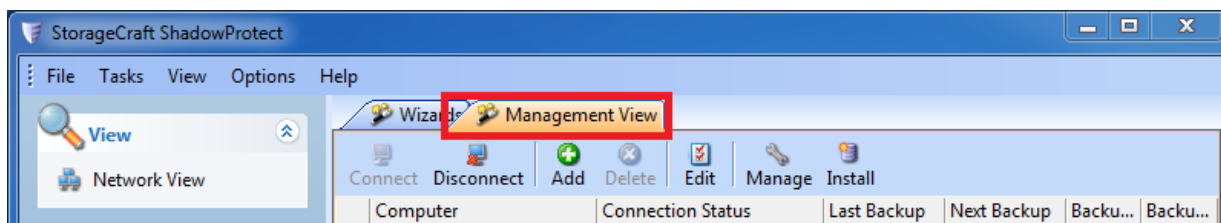
- Disable automatic defrag in the task manager.
- Do a defrag one time before the first full backup.
- Add exceptions to the firewall for ShadowProtect (or turn the firewall off).
- Set the **ShadowProtect Service** to run as the highest level admin, domain, or local admin. (This setting is based on whether the protected server is in a domain or not.)
- Disable **Shadow Copies** on each of the volumes to be backed up.

### 5. Configure ShadowProtect

- a) On the BDR desktop, click the **ShadowProtect** icon to open the *ShadowProtect Console*.

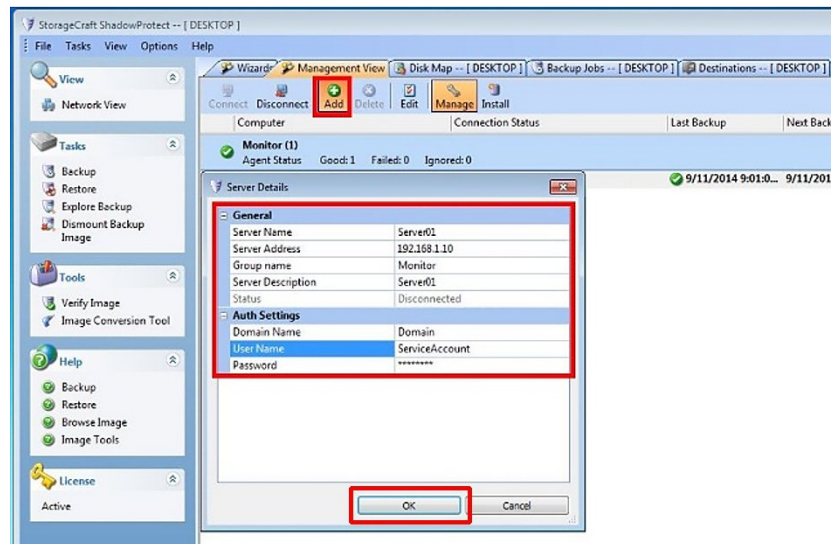


- b) Click the **Management View** tab.



## Add additional managed computers to this console

1. To add computers which already have a ShadowProtect agent installed to this *Management View* console, click the **Add** icon.
2. Enter data in the fields for **Server Name**, **Server IP Address**, **Group name**, **Server Description** (this can be the server name), **Domain** (or server name), **User Name**, and **Password**.
3. When all fields are completed, click **OK**.



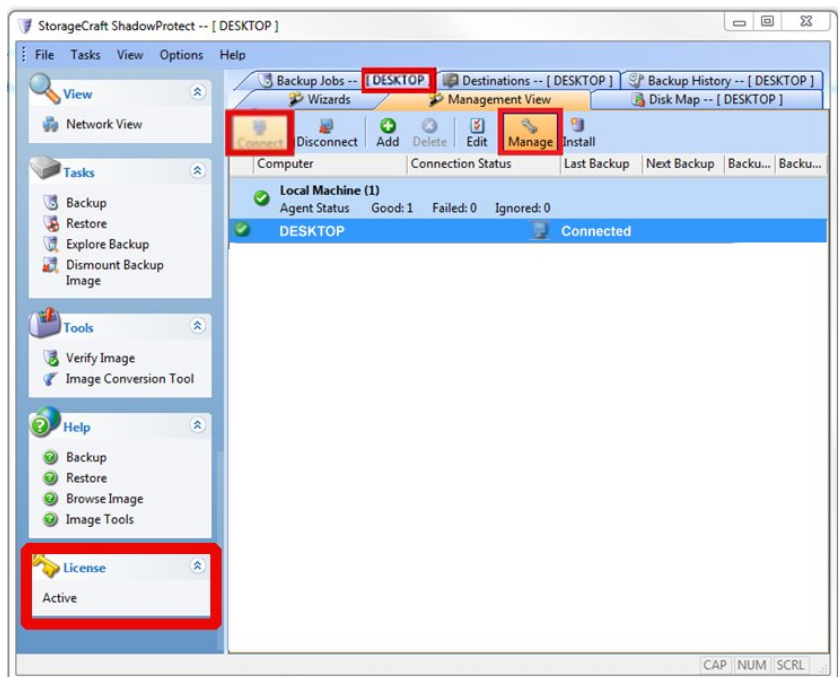
The newly added computers which have a previously-installed ShadowProtect agent will now display in the list on this console.

## Connect and manage from this console

1. Highlight the desired computer and click **Connect**.
2. After the computer shows **Connected**, click **Manage**.

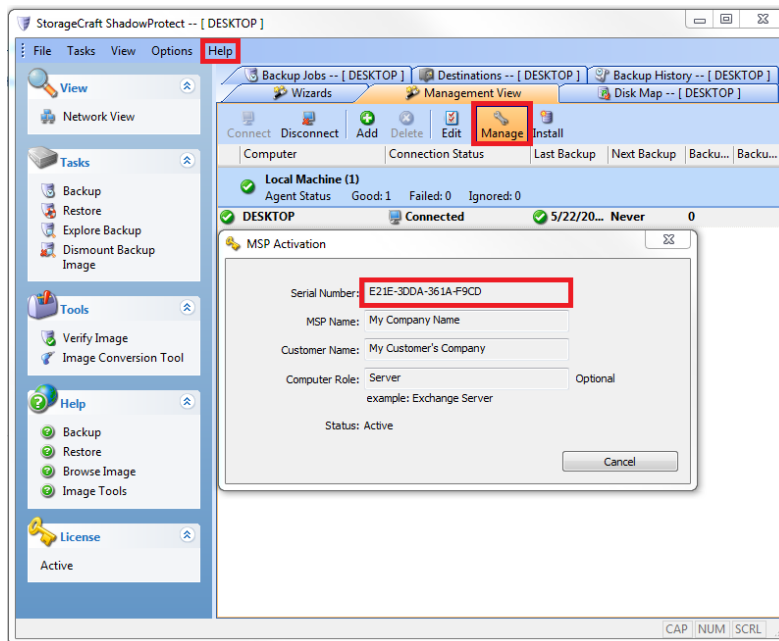
**Note:** When you are actively managing a computer, that **computer's name** appears in new tabs along the top and in the Window banner.

Also, notice that the **license status** for the server you are currently managing is now shown in the bottom left corner.



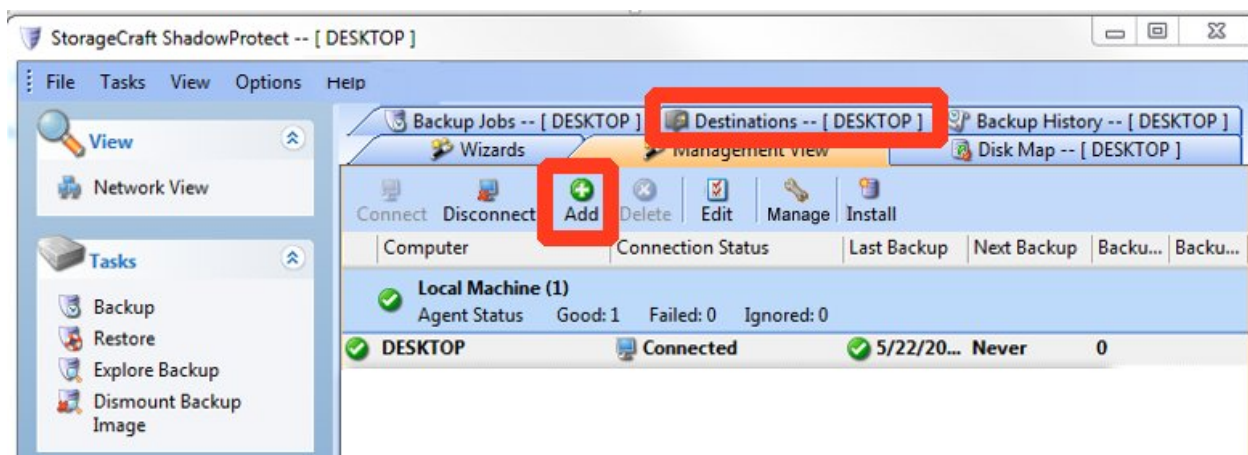
## Activate a license

1. To activate a license, first **Manage** the desired computer.
2. Next, click **Help**; then, click **Product Activation**.
3. Now paste the **ShadowProtect Key** (previously provisioned on the eFolder Web Portal) in the **Serial Number** field.

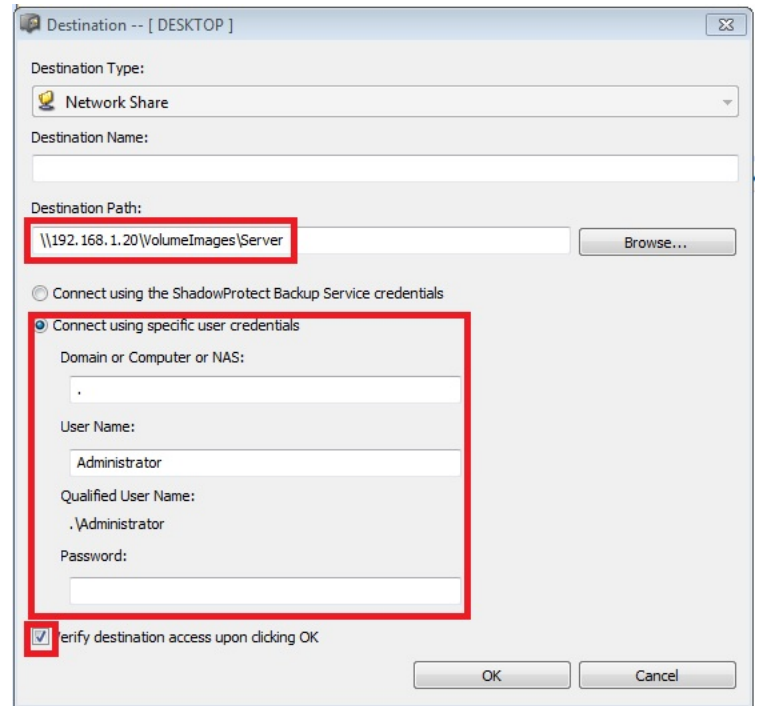


## Create a new destination

1. Before creating a new job, click on the **Destinations** tab.
2. Then click the **Add** button to create a new destination.



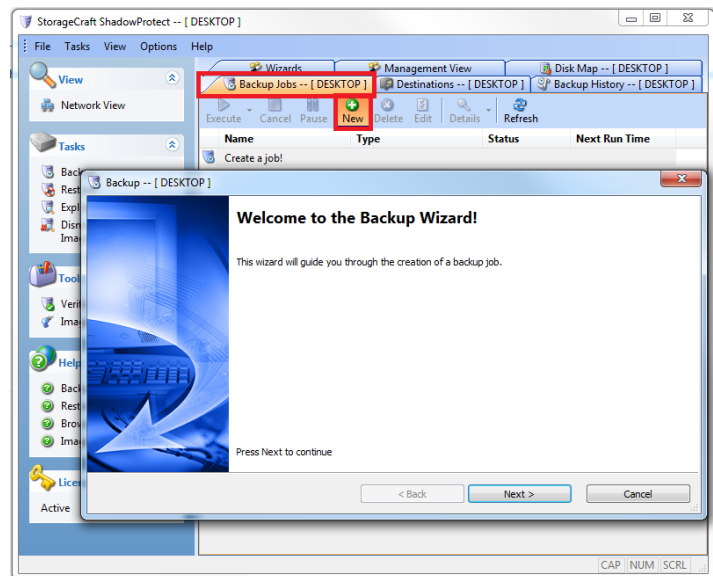
3. Enter the **destination path** and the **ShadowProtect credentials** in their respective fields.
4. Next, verify that the checkbox is clicked for the **Verify destination access upon clicking OK** field; then, click **OK**.



## Create a new backup job

1. To create a new backup job, click the **Backup Jobs** tab; then, click the **New** icon to start the Backup Wizard.

Click **Next** to continue.

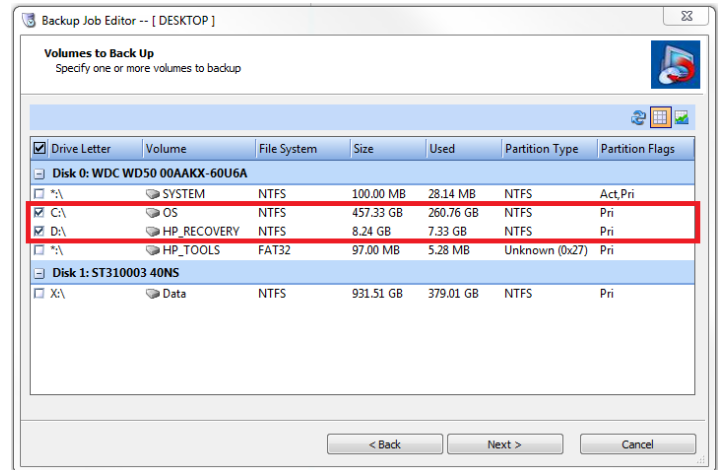




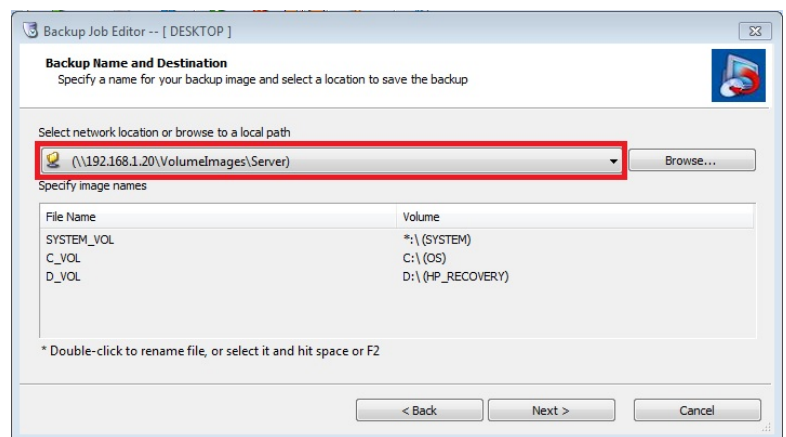
2. Select the volume(s) for which you want to create images. Click **Next** to continue.

**Note:** It is important that the volumes be together in the same job.

If you are running Exchange or SQL and the logs are not on the same volume as the application database, the logs will not truncate **unless the volumes are together in the same backup job.**



3. If the target path is on a network share, click the **down arrow** and select the destination previously created. Click **Next** to continue.



4. On the *Specify backup schedule* screen:

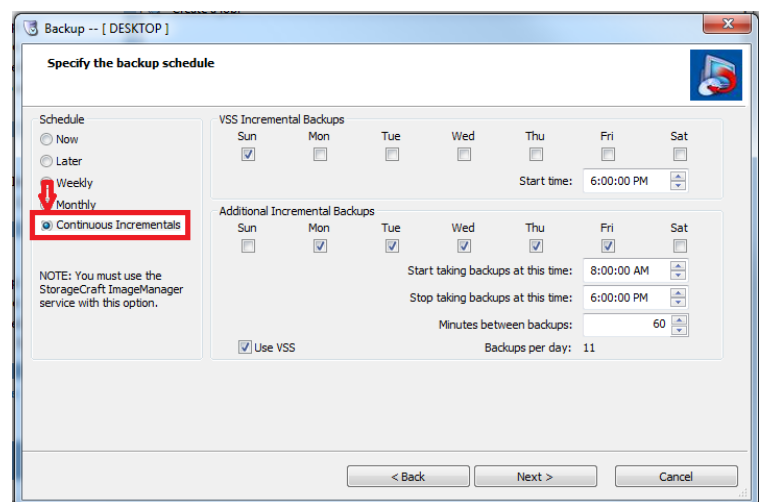
- a. Select **Continuous Incrementals**.

- b. Set the desired schedule.

The schedule on the top row will run a single incremental backup.

The schedule on the second row will run multiple backups according to the set schedule.

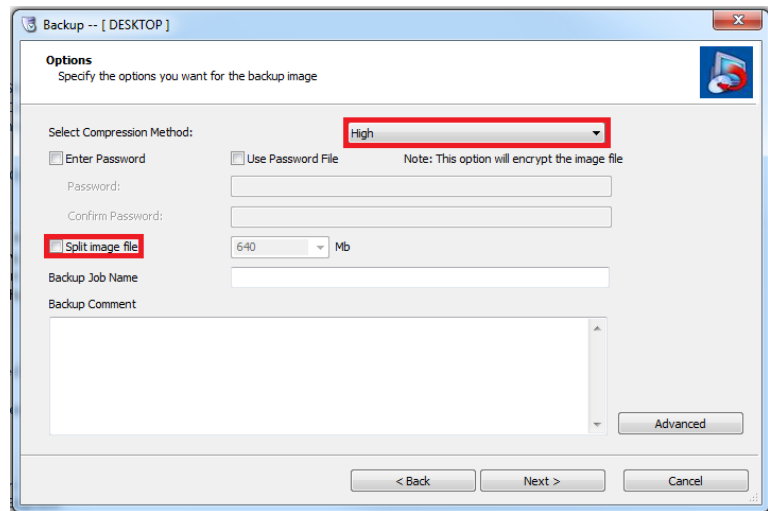
- c. Click **Next** to continue.



5. On the *Options* screen:
  - a. We recommend that you select the **High** compression method.

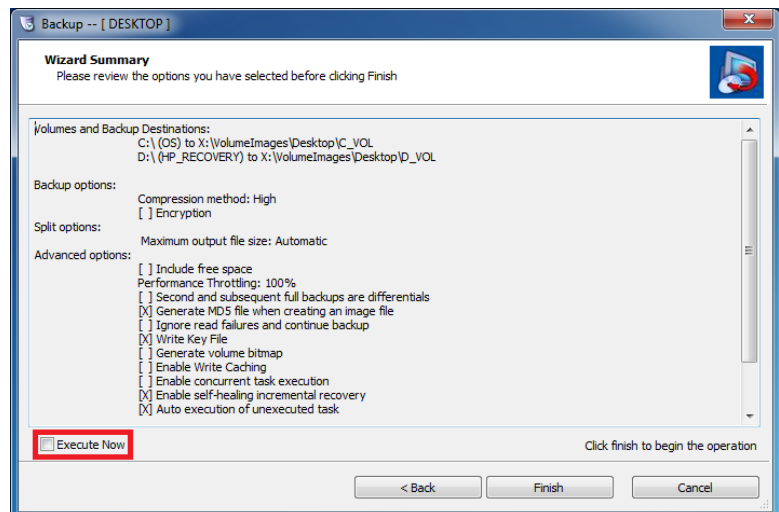
**High** has about a 50% compression while **Standard** has about a 40% compression.

- b. Confirm that the **Split image file** check box is unchecked (do not split the image files).
  - c. Click **Next** to continue.




6. On the *Wizard Summary* page:
  - a. Leave the **Execute Now** checkbox *unchecked*. This setting will run the initial backup at the next scheduled time.
  - b. Click **Finish** to complete the new backup job setup.

**Note:** If you wish to run the backup immediately, select the **Execute Now** checkbox.



## Configuring ImageManager

ShadowProtect uses forward deltas that require periodic management. **ImageManager** is a utility that consolidates hourly incrementals into daily incrementals, daily incrementals into weekly incrementals, weekly incrementals into monthly incrementals, and monthly incrementals into rolling incrementals.


 **TIP:** You will only need to install **ImageManager** on the computer that is physically storing or managing the volume images. Typically, this is the same computer that is also using **eFolder Online Backup Manager** to transfer the volume images to the cloud.

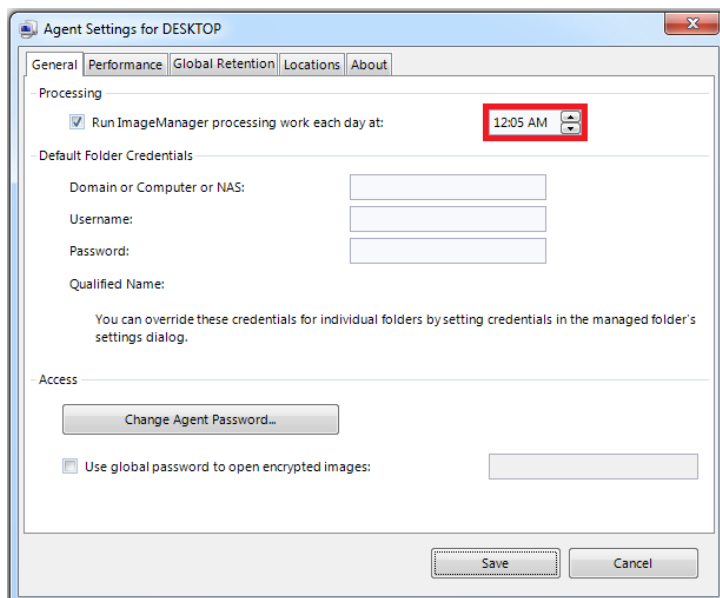
The strategy for efficient off-site disaster recovery backups is to have eFolder back up only the daily, monthly, and rolling collapsed incrementals. The hourly and weekly incrementals will *not* be backed up remotely.

The first step after installing **ImageManager** is to configure the settings.

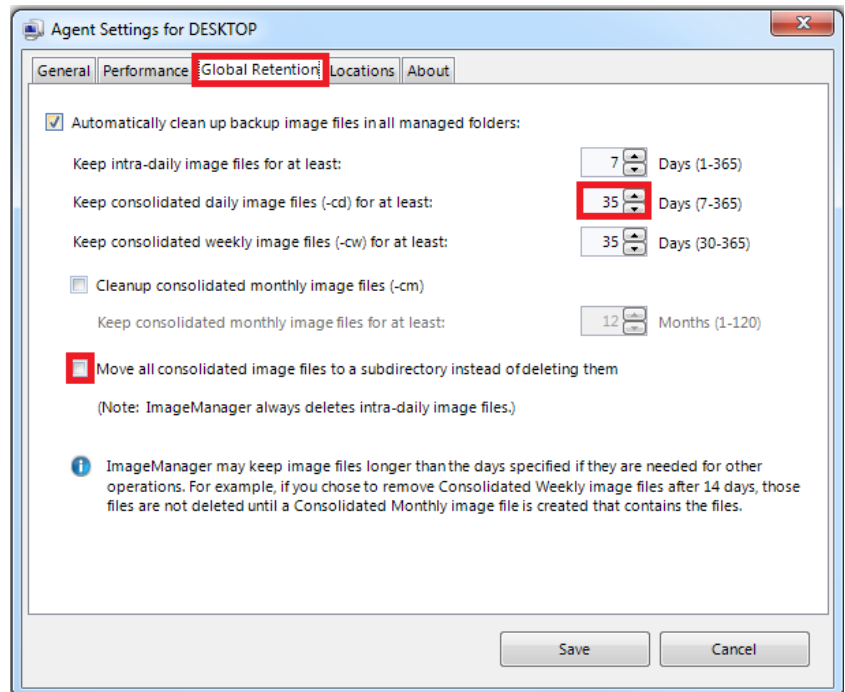
1. Click the **ImageManager** icon on the desktop.



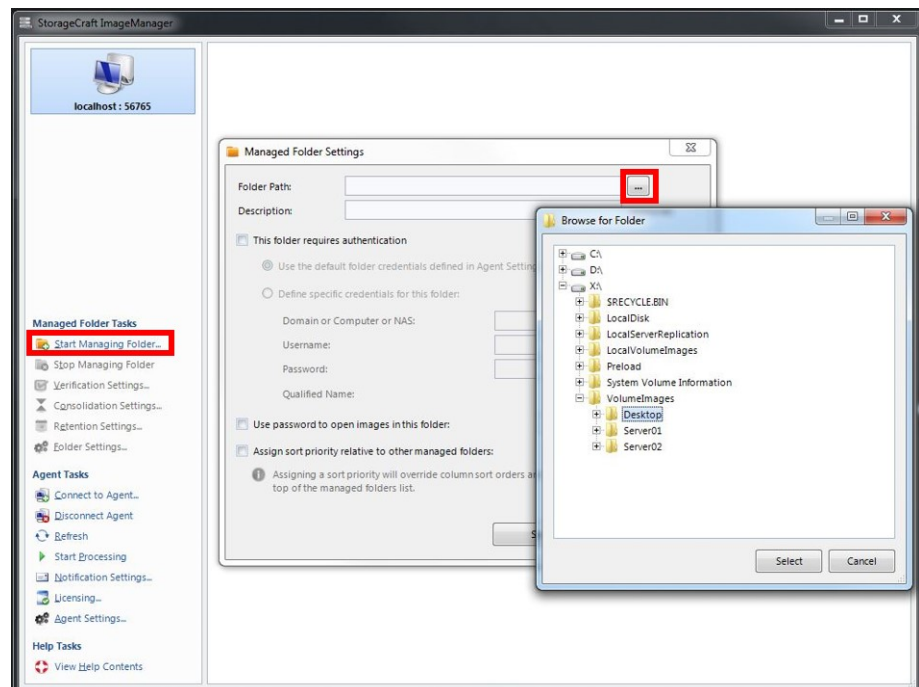
2. Next, click the  **Agent Settings...** button near the bottom left corner.
3. Verify that ImageManager is set to run shortly after midnight, as in this example where it is set to run at *12:05 a.m.*



4. Click the **Global Retention** tab.
  - a. Verify that **Keep consolidated daily image files** is set to at least 35 days.
  - b. Clear the last checkbox, **Move all consolidated image files to a subdirectory instead of deleting them**. This checkbox should be unchecked.
  - c. Finally, click **Save**.

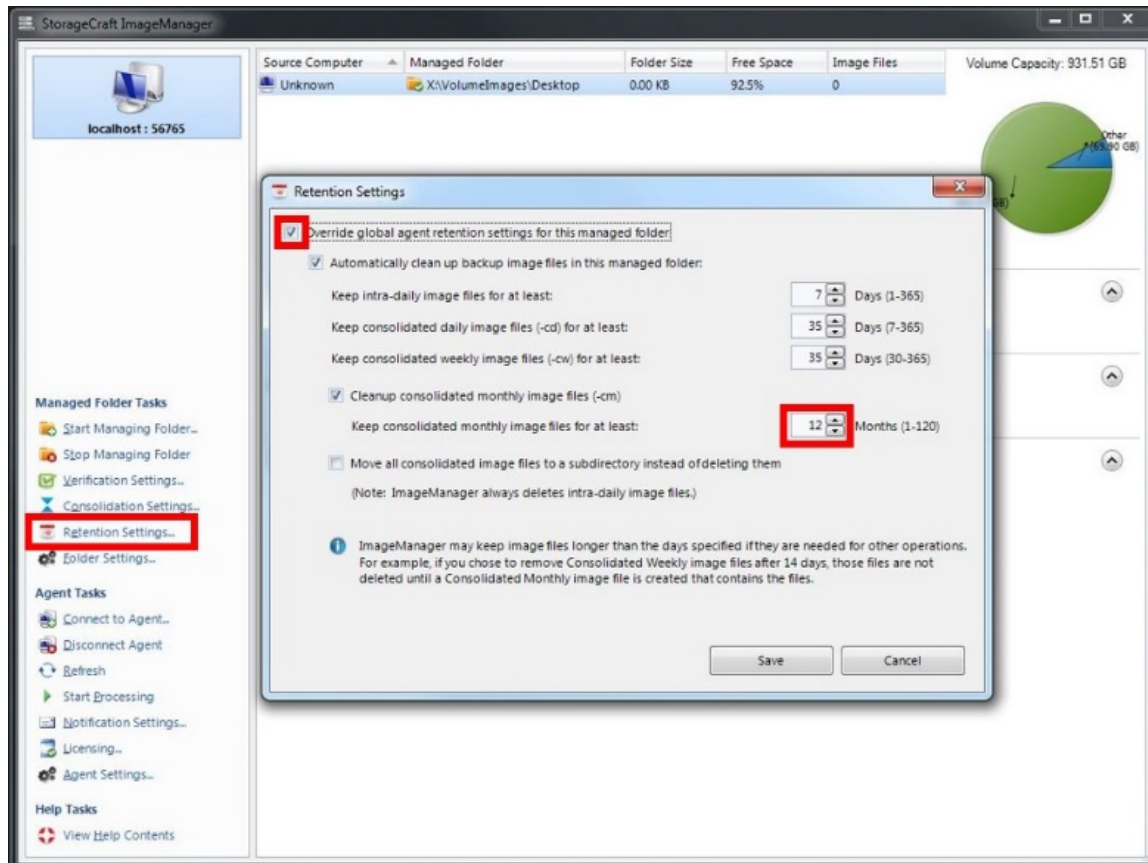


5. Next, click **Start Managing Folder**.
  - a. Browse to the folder that contains the ShadowProtect image files that you want to manage.
  - b. Repeat this step for each folder that you want to manage.



## Customizing retention settings

If you have a system which requires a customized retention setting (different from the global default), you can adjust retention values manually.



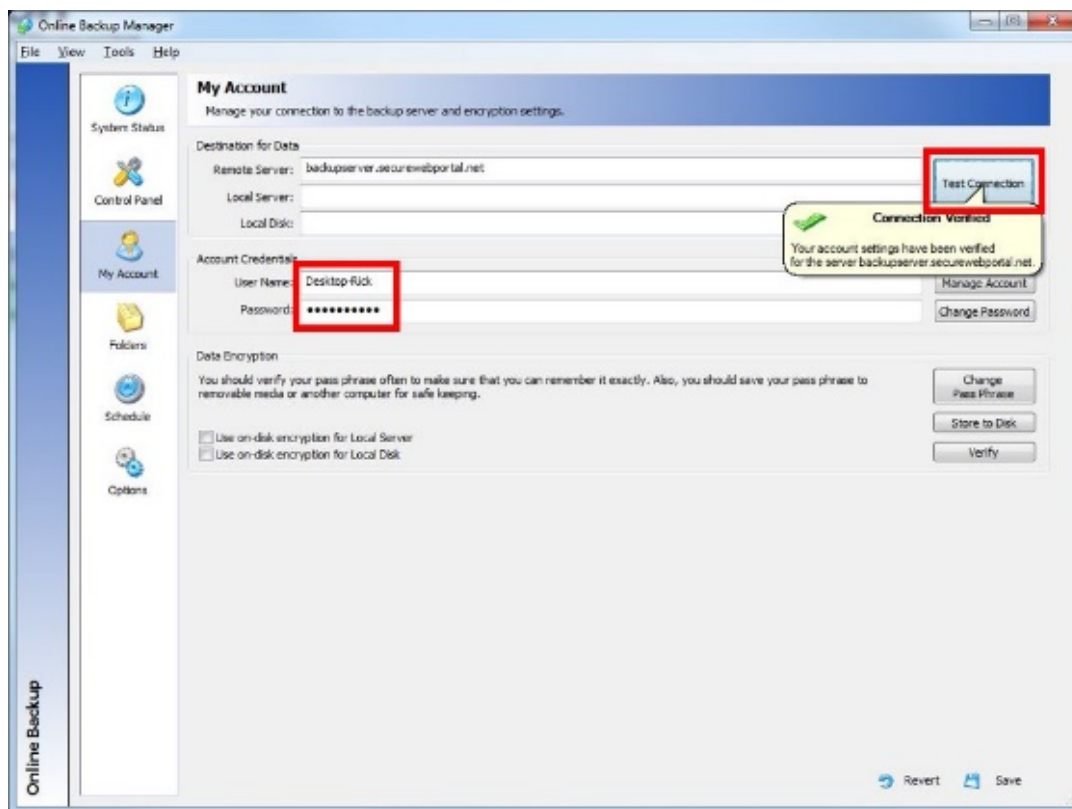
- Highlight the desired folder.
- Select **Retention Settings** on the left side.
- Click the checkbox **Override global agent retention settings for this managed folder**.
- Adjust the desired settings.
- Click **Save** when the new settings are complete.

## Configuring eFolder Online Backup Manager

1. To configure the Backup Manager, click the **Online Backup** icon on the BDR desktop.

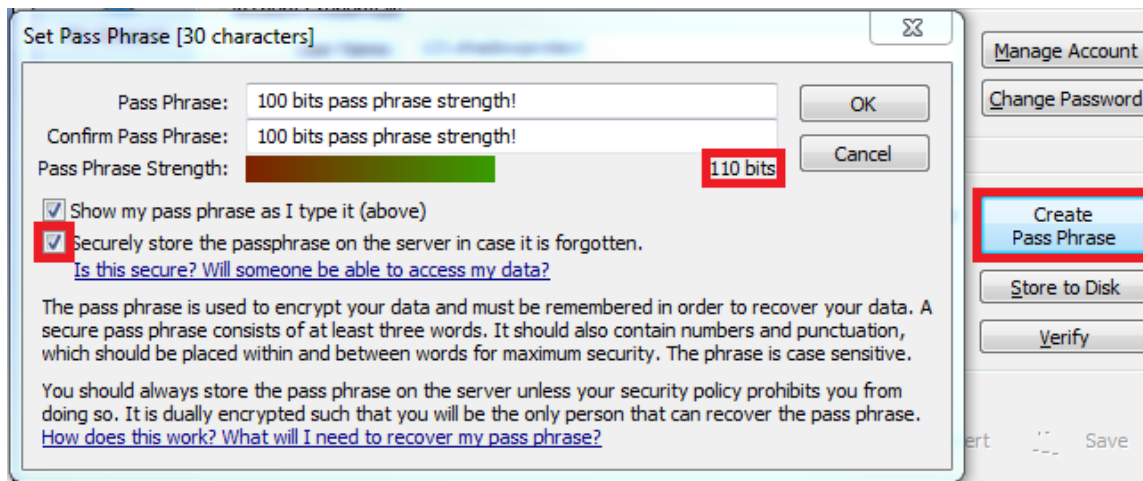


2. Select the **My Account** tab.
  - a. Enter the **User Name** and **Password** for the desired eFolder account.
  - b. Click the **Test Connection** button on the top right.

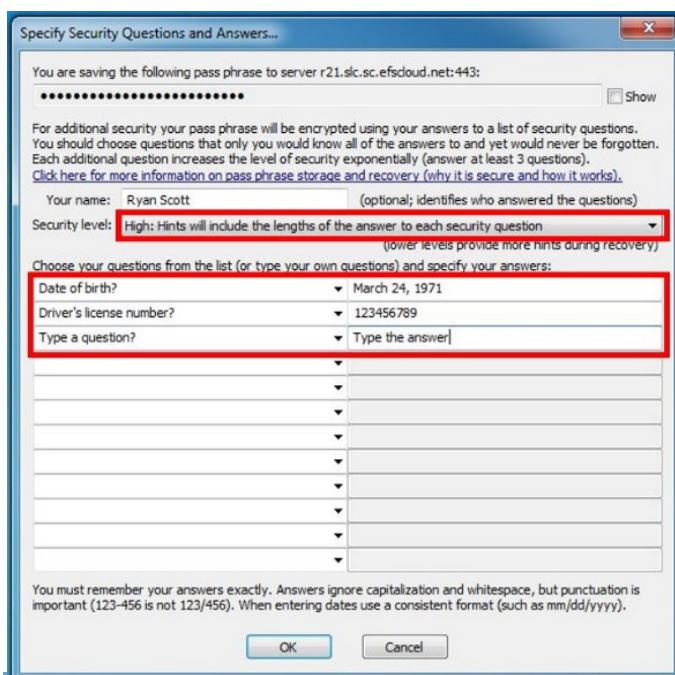


**Note:** Contact Technical Support if the *Connection Verified* window does *not* appear.

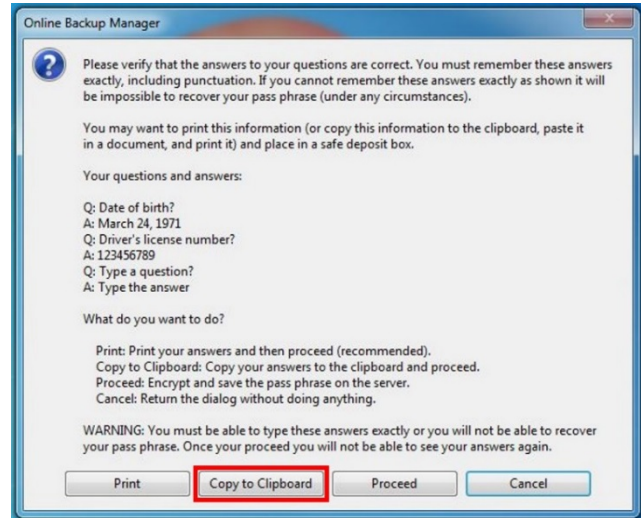
3. To create a pass phrase:
  - a. Click **Create Pass Phrase**.
  - b. Enter a pass phrase that has a strength of 100 bits or more.
  - c. Verify that the checkbox **Securely store the passphrase on the server in case it is forgotten** is checked.



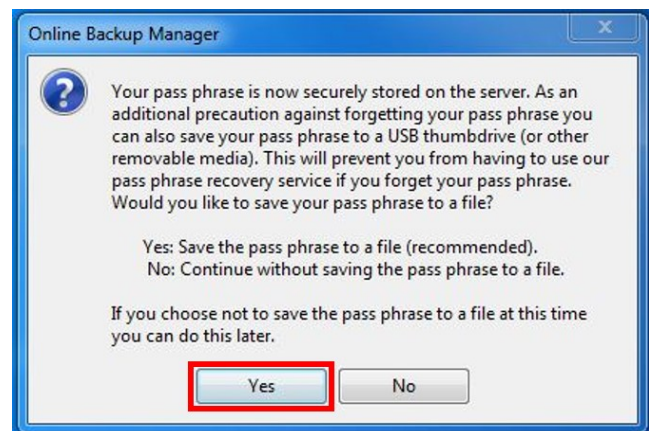
4. To store the **Pass Phrase** in the eFolder Cloud, create at least three questions and answers. You can use the predefined questions or create your own. Then, set the desired **security level** in the **Security level** field.



5. You can copy the questions and answers to the clipboard so you can paste them into your password vault or other location by clicking **Copy to Clipboard**.

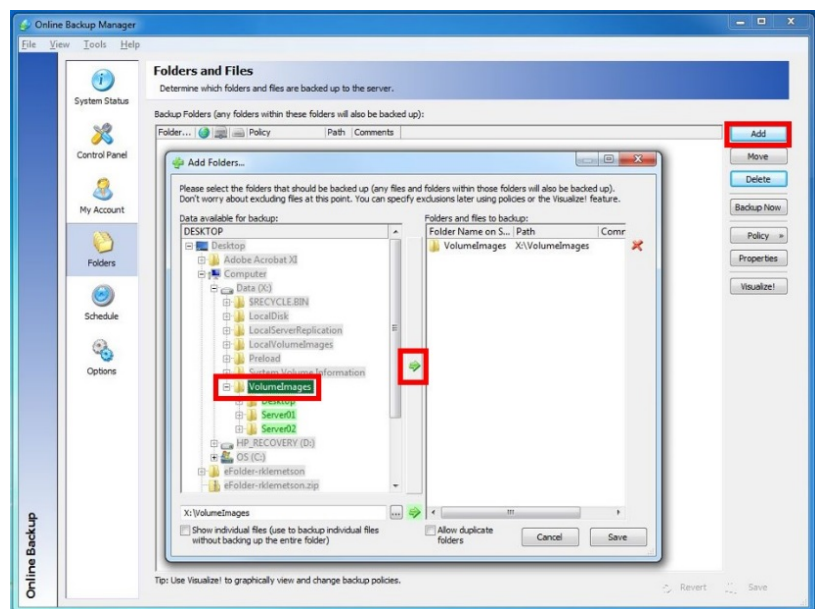


6. You can save the **Pass Phrase** to a text file on a removable drive, if desired, by clicking **Yes**.



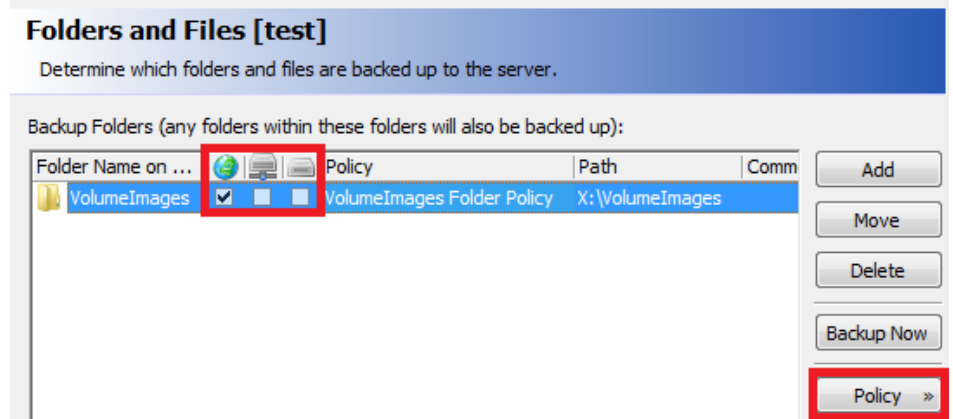
7. To add the *Volumelimages* folder to the folders that will be backed up:

- a) Click the **Folders** button.
- b) Click **Add**.
- c) Browse to the *X:\volumelimages* folder.
- d) Click the **green arrow** to move the folder to the right side of the screen.
- e) Click **Save**.

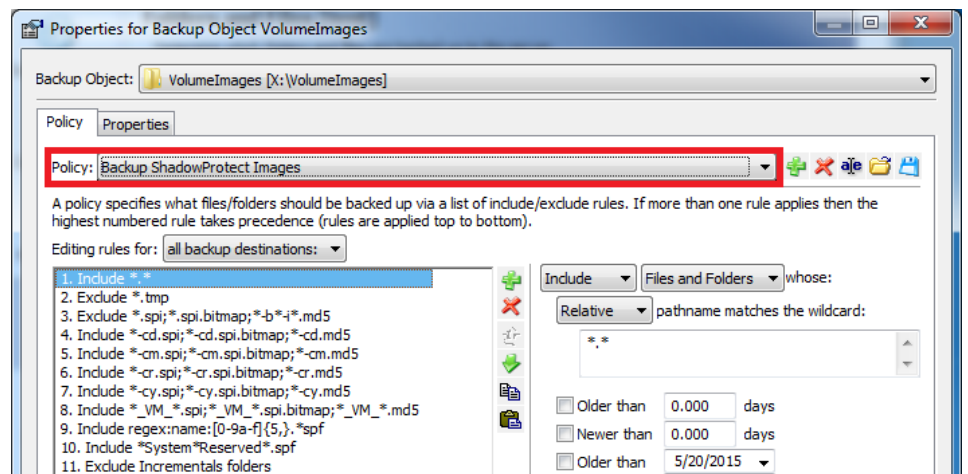




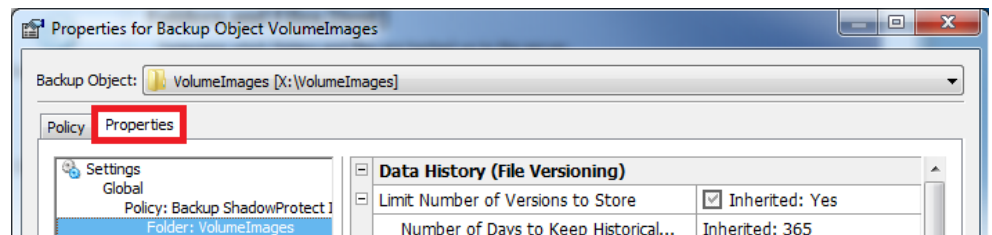
8. Clear the checkboxes for the columns that are *not* configured for backups. The icons in the three columns indicate **Cloud Backup**, **Local Server**, and **Local Disk**, from left to right.
  - a. Highlight the *VolumeImages* folder.
  - b. Click **Policy** on the right side.
  - c. Select **Edit Policy**.



9. Select **Backup ShadowProtect Images** from the *Policy* drop down menu.



10. Click the **Properties** tab.

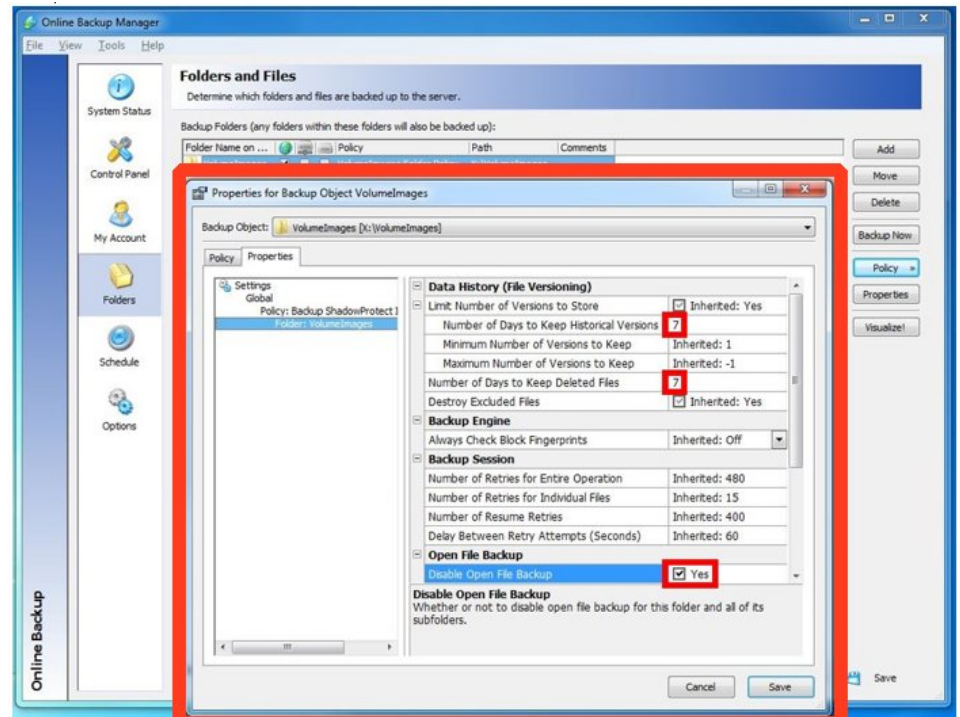


10. On the *Properties* tab:

- a. Change the **Number of Days to Keep Historical Versions** to **7**.

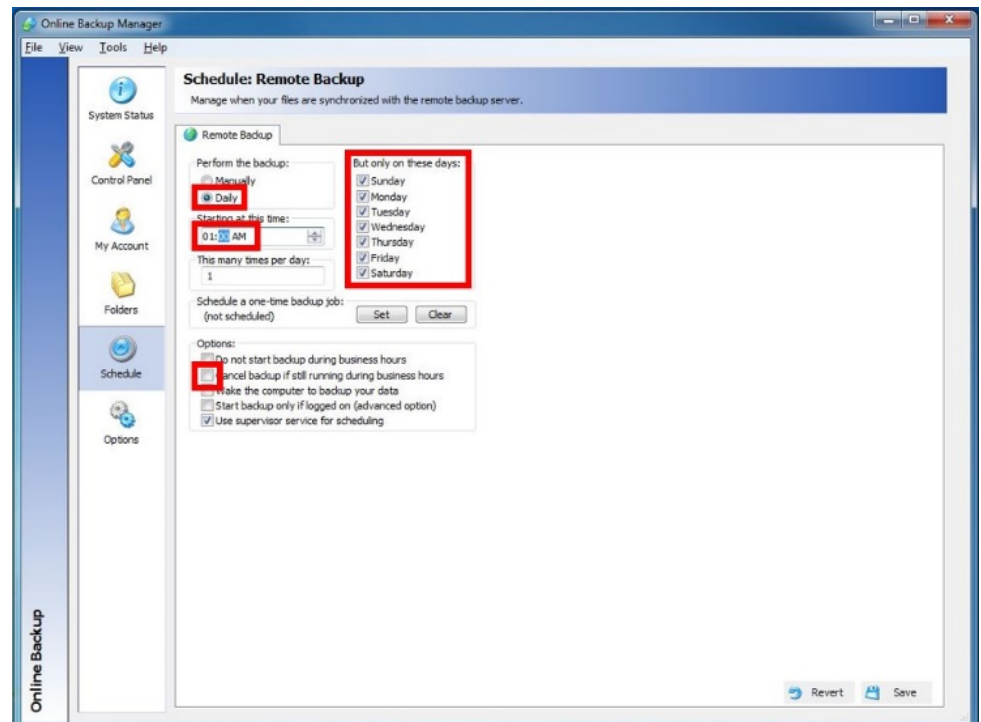
This will also automatically change the **Number of Days to Keep Deleted Files** to **7**.

- b. Change **Disable Open File Backup** to **Yes**

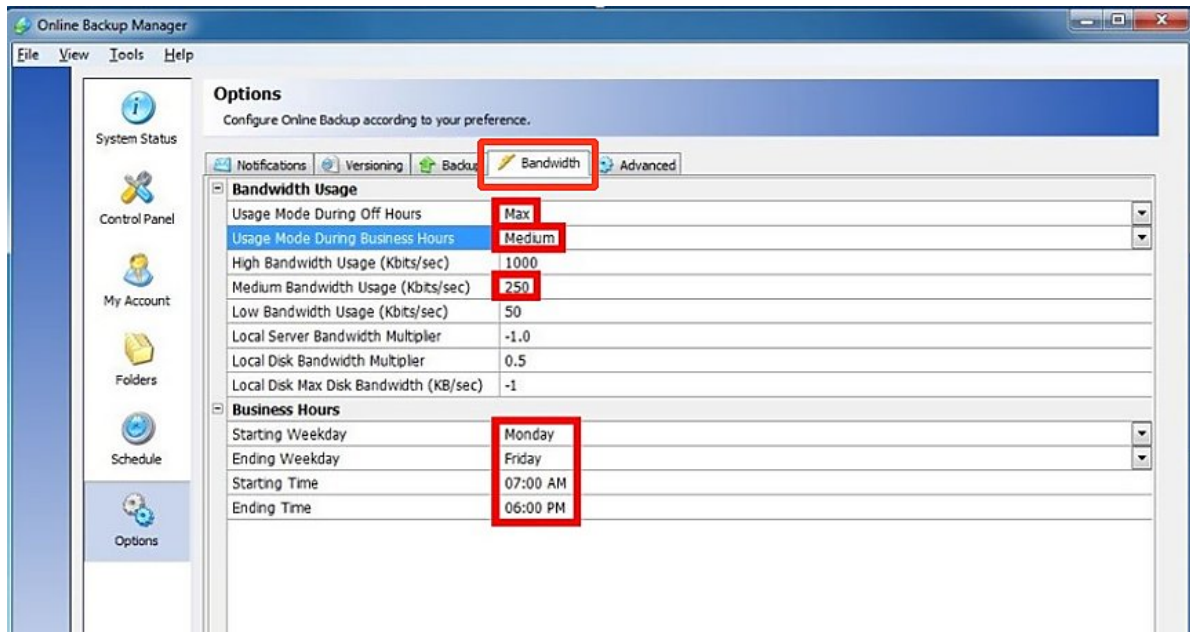


12. Click **Schedule** on the left panel.

- a) Verify that **Daily** is selected.
- b) Set the time to about **1:00 AM** and verify that all seven days are selected.
- c) Verify that the checkbox **Cancel backup if still running during business hours** is cleared. This checkbox should *not* be checked.



13. Click **Options** on the left panel. Then click the **Bandwidth** tab at the top.



- Set **Business Hours** to an hour before and after normal working hours for your customer's employees.
- Set the **Usage Mode During Business Hours** field to **Medium**.
- Then set **Medium Bandwidth Usage** to 25% of the customer's upload speed.
- Set the **Usage Mode During Off Hours** field to **Max**.

**Note:** If the client needs the Internet after hours, adjust these settings:

- Set **Usage Mode During Off Hours** to **High**.
- Set the **High Bandwidth Usage** to 75% of the customer's upload speed.

## Create a preload (seed) drive

- To request a preload (seed) drive form eFolder:  
[Request a Preload \(Seed\) Drive Form](#)
- For help completing the request form:  
[How to request a preload \(seed\) drive](#)
- To create a ShadowProtect preload (seed) drive to ship to the eFolder data center:  
[How to create a ShadowProtect preload \(seed\) drive:](#)

## Restoring, migrating, or virtualizing servers

To restore servers (or migrate servers to new hardware) when you still have access to the local ShadowProtect volume images, follow the normal ShadowProtect bare-metal restore procedure using the bootable restore environment. If you have been backing up your volume images with eFolder local or remote backups, you can use eFolder local or remote restore to restore your .SPF and .SPI files if they ever become damaged.

You can also use StorageCraft **VirtualBoot** to quickly virtualize any of your backup recovery points that are local. You can use the **eFolder Continuity Cloud** to virtualize your ShadowProtect backups in our cloud, if you have previously signed up for this service. Contact your Account Manager for detailed instructions.

Files that are remotely backed up to eFolder's data center are protected by eFolder's extremely rigorous data integrity procedures. All remotely backed up data has an embedded cryptographic fingerprint that is verified upon restore, certifying the restored file is exactly identical to the backed up file. Additionally, we use block-level checksums to automatically guard against and safely repair any silent data corruption that occurs with any electronic storage device. eFolder also verifies the MD5 checksum that was generated by ShadowProtect to ensure that the file that was backed up was not damaged. Your files are safe with us. If your local "chain" of ShadowProtect incrementals becomes damaged, you can be assured that eFolder will have a good, undamaged copy ready for restore.

**Note:** Use the notification and alerting features in the eFolder Web Portal so that you will be alerted if any local ShadowProtect or cloud backups fail and need attention.

### Restoring individual files

The eFolder restore wizard allows you to easily restore files and folders (for data backed up directly with the eFolder Backup Manager) simply by logging in, checking off the data you want to restore, choosing the point-in-time version, and choosing where you want to restore the data.

## Recovering from a disaster

To recover from complete data loss at the local site:

1. Provision appropriate bare-metal or virtual machines for the server(s) you need to restore. Make sure there is enough disk space to fully contain the restored volumes.
2. Use eFolder Web Access (select **Online Access** on the **Web Access** option on the main menu bar in the [eFolder Web Portal](#)) to download the .spf and all .spi files for the relevant OS and application volume image(s) to a portable USB disk or network share accessible from the ShadowProtect bootable restore environment.

**Note:** Be sure to *uncheck* the **Include the deleted date and time in the restored filename** option, so that the restored files are named properly.

3. Use the ShadowProtect bootable restore environment to deploy the volume images to the new bare-metal server or virtual machine. Or, if you have ShadowProtect 4 or 5 and used ShadowProtect to backup all volumes of your server, you can also use the VirtualBoot feature to instantly boot a virtual machine from the most current \*.spi file.
4. With the server and critical applications fully restored, login and immediately change the eFolder schedule to manual (if eFolder is configured on the machine).
5. Start the eFolder File Manager (by clicking the **Control Panel** tab of the Backup Manager and selecting **File Manager**) to restore any remaining file-based data as needed.
6. With all data fully restored, set the eFolder backup schedule back to Weekly.

## Additional assistance

We will assist you any way that we can. Please submit questions to [support@efolder.net](mailto:support@efolder.net), call us at 800-352-0248, or browse our Knowledgebase at <https://secure.efoldering.com/support/kb/>



The People Behind Your Cloud