eFolder BDR for ShadowProtect
Solution Guide and Best Practices

Last Updated May 2015

Best Practices

This guide will walk you step-by-step through the process of combining the eFolder and StorageCraft products.

Process Overview

First, provision eFolder accounts for computers that will be backing up data remotely, and install ShadowProtect on those computers requiring volume-level backups. Next, configure ShadowProtect to perform volume backups of your OS and critical server applications. Finally, configure eFolder to backup other files and your ShadowProtect volume backup images.

If you have questions, wish to deviate from the guidelines, or have a different version of ShadowProtect, please contact us first at support@efolder.net.

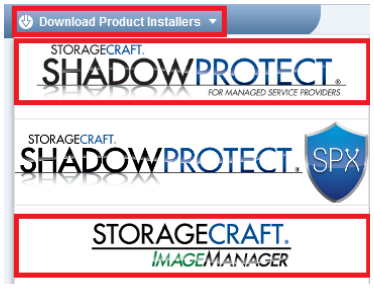
Assess Requirements, Provision Accounts, and Install Software

1. First, assess the backup requirements of your customer. Identify the following:

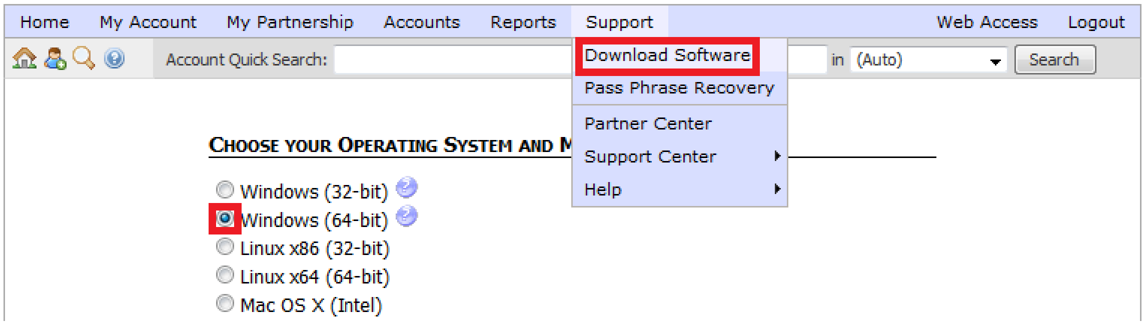
- Critical application servers, such as Exchange, SQL, and SharePoint
- The Recovery Point Objective for these critical applications
- Where to store volume backup images
- Data that must be retained for years, because of compliance or company policy
- Files that users may want to restore individually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

2. Create the account as needed on the eFolder portal – see Create an account using the New Account Wizard video - https://backup.securewebportal.net/efolder/learningcenter/How%20to%20video%20snippets/Create%20an%20account%20using%20the%20New%20Account%20Wizard/Create%20an%20account%20using%20the%20New%20Account%20Wizard.mp4

3. Prior to beginning, verify that you have the correct version of ShadowProtect and ImageManager installed. The "Download Product Installers" link is available in the top left corner of https://msp.storagecraft.com/msp/


Download Product Installers
STORAGECRAFT. SHADOWPROTECT. FOR MANAGED SERVICE PROVIDERS
STORAGECRAFT. SHADOWPROTECT. SPX
STORAGECRAFT. IMAGEMANAGER

4. Download eFolder Online Backup Manager, if needed, by hovering over Support on the eFolder portal and selecting Download Software. Select the desired version.



CHOOSE YOUR OPERATING SYSTEM AND M

○ Windows (32-bit)
● Windows (64-bit)
○ Linux x86 (32-bit)
○ Linux x64 (64-bit)
○ Mac OS X (Intel)

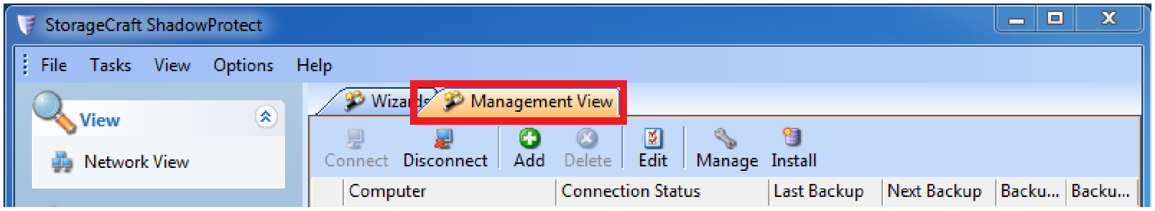
Scroll to the bottom of the page and click the check box to agree and then click Download.

Configure ShadowProtect

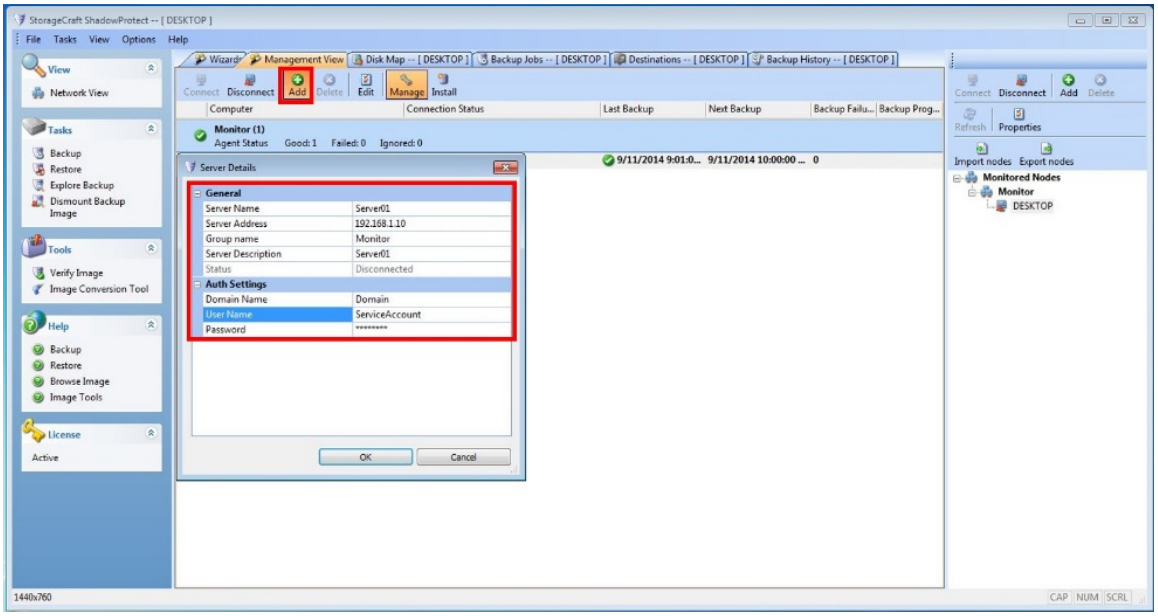
Install ShadowProtect on each server that requires volume backups. Do not use the PUSH install included with ShadowProtect, instead use the installable package and install the COMPLETE package on your agents being backed up. Note – the server must be rebooted prior to performing the first full backup.

1. Prior to configuring ShadowProtect, complete the following preparation steps:
   - Disable automatic defrag in task manager
   - Do a defrag one time before first full backup
   - Add exceptions to firewall for ShadowProtect or Turn firewall off
   - Set the ShadowProtect Service to run as the highest level admin, domain or local admin, depending if protected server is in a domain or not
   - Disable Shadow Copies on each of the volumes to be backed up
2. To begin, on the BDR, click the ShadowProtect icon on the desktop to open the *ShadowProtect Console*.

3. Click the Management View tab.



4. To add the additional computers to this Management View console for which you have already installed the ShadowProtect agent, click the Add icon. Add the *Server Name, Server IP Address, Group name of Monitor, Server Description (can be the server name)* and the *Domain (or server name), User Name*, and *Password*.

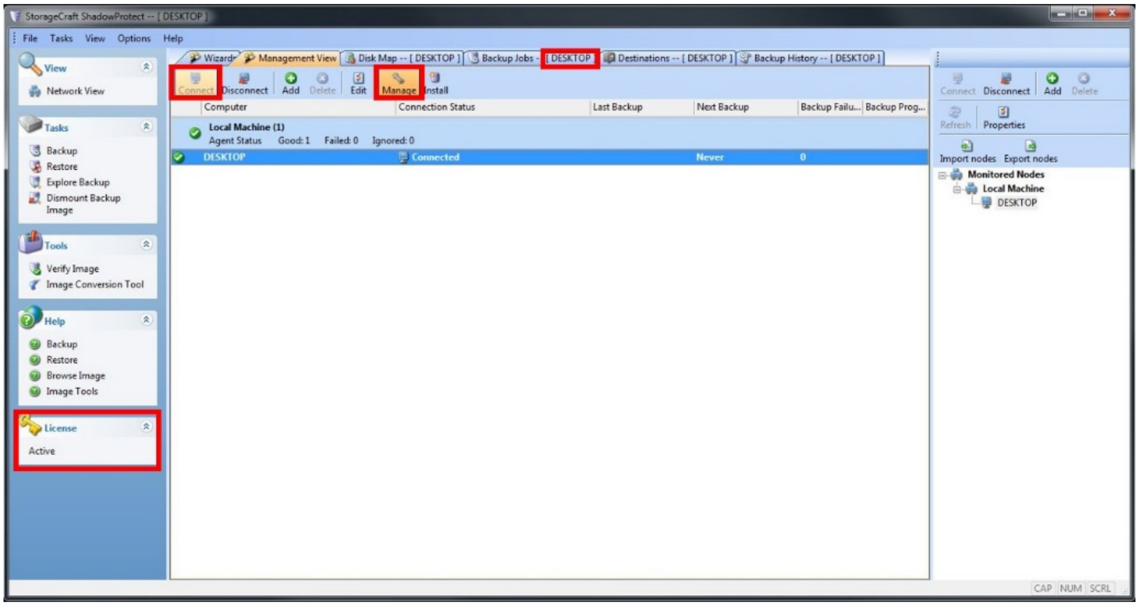


Computer	Connection Status	Last Backup	Next Backup	Backup Failu...	Backup Prog...
Monitor (1) Agent Status Good: 1 Failed: 0 Ignored: 0					
		9/11/2014 9:01:0...	9/11/2014 10:00:00 ...	0	

General	
Server Name	Server01
Server Address	192.168.1.10
Group name	Monitor
Server Description	Server01
Status	Disconnected
Auth Settings	
Domain Name	Domain
User Name	ServiceAccount
Password	********

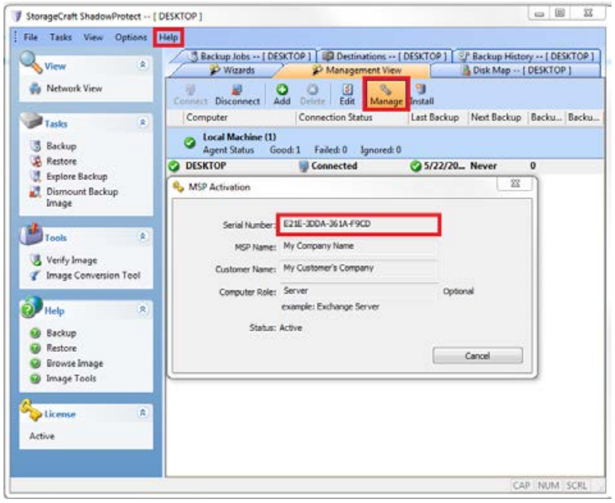
The computers are now displayed in the list.

5. Highlight the desired computer and click Connect. After the computer shows Connected, click Manage. Note: When you are managing a computer, the computer name appears in the new tabs along the top and in the Window banner. In addition, the license status for the server that you are managing is shown in the bottom left corner.



Computer	Connection Status	Last Backup	Next Backup	Backup Failu...	Backup Prog...
Local Machine (1) Agent Status Good: 1 Failed: 0 Ignored: 0					
DESKTOP	Connected		Never	0	

6. To activate the license, Manage the desired computer, click Help and then click Product Activation. Paste the ShadowProtect Key that you provisioned on the eFolder Portal.



Computer	Connection Status	Last Backup	Next Backup	Backu...
Local Machine (1) Agent Status Good: 1 Failed: 0 Ignored: 0				
DESKTOP	Connected	5/22/20...	Never	0

MSP Activation

Serial Number: E21E-3DDA-361A-F9CD

MSP Name: My Company Name

Customer Name: My Customer's Company

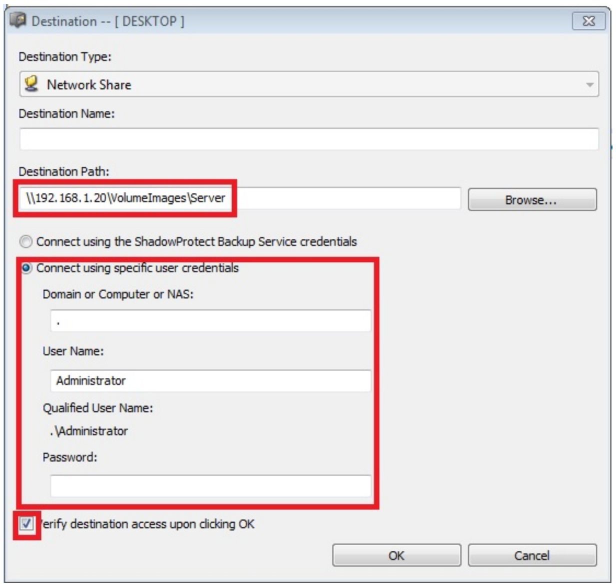
Computer Role: Server Optional

example: Exchange Server

Status: Active

Cancel

7. Before creating the new job, first click on the Destination tab. Click Add button to create a new destination. Enter the UNC path, credentials, and verify that the check box is clicked for "Verify destination access upon click OK", then click OK.


Destination -- [DESKTOP]

Destination Type: Network Share

Destination Name:

Destination Path: \\192.168.1.20\VolumeImages\Server Browse...

○ Connect using the ShadowProtect Backup Service credentials

● Connect using specific user credentials

Domain or Computer or NAS: .

User Name: Administrator

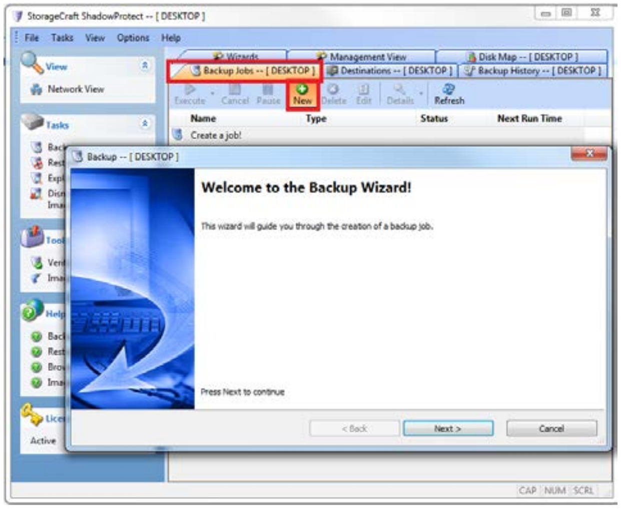
Qualified User Name: .\Administrator

Password:

☑ Verify destination access upon clicking OK

OK Cancel

8. To create a new backup job, click the Backup Jobs tab and then click the New icon to start the Backup Wizard.



Name	Type	Status	Next Run Time
Create a job!			

Backup -- [DESKTOP]

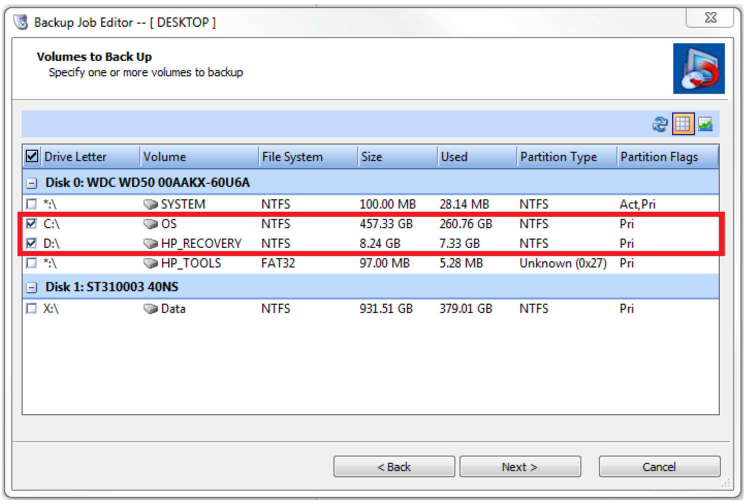
Welcome to the Backup Wizard!

This wizard will guide you through the creation of a backup job.

Press Next to continue

< Back Next > Cancel

9. Select the volume(s) for which you want to create images. Note – if the Exchange or SQL logs are not on the same volume as the application database, it is important that the volumes be together in the same backup job, otherwise the logs will not be truncated.

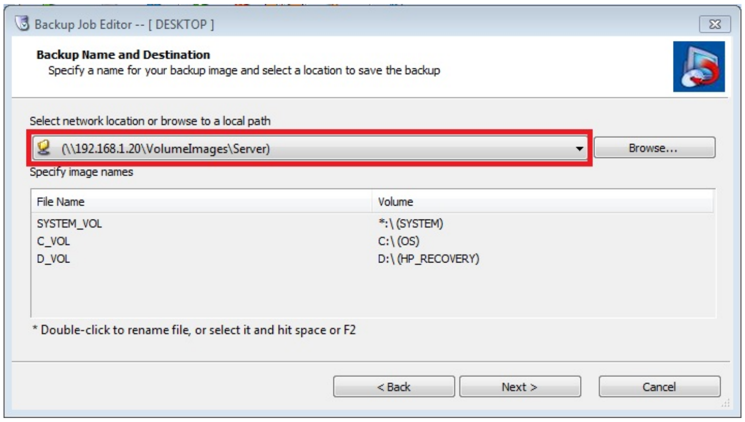


Backup Job Editor -- [DESKTOP]

Volumes to Back Up
Specify one or more volumes to backup

☑ Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
⊟ **Disk 0: WDC WD50 00AAKX-60U6A**						
☐ *:\	SYSTEM	NTFS	100.00 MB	28.14 MB	NTFS	Act,Pri
☑ C:\	OS	NTFS	457.33 GB	260.76 GB	NTFS	Pri
☑ D:\	HP_RECOVERY	NTFS	8.24 GB	7.33 GB	NTFS	Pri
☐ *:\	HP_TOOLS	FAT32	97.00 MB	5.28 MB	Unknown (0x27)	Pri
⊟ **Disk 1: ST310003 40NS**						
☐ X:\	Data	NTFS	931.51 GB	379.01 GB	NTFS	Pri

10. If the target path is on a network share, click the down arrow and select the destination that was created in step 5.



Backup Job Editor -- [DESKTOP]

Backup Name and Destination
Specify a name for your backup image and select a location to save the backup

Select network location or browse to a local path

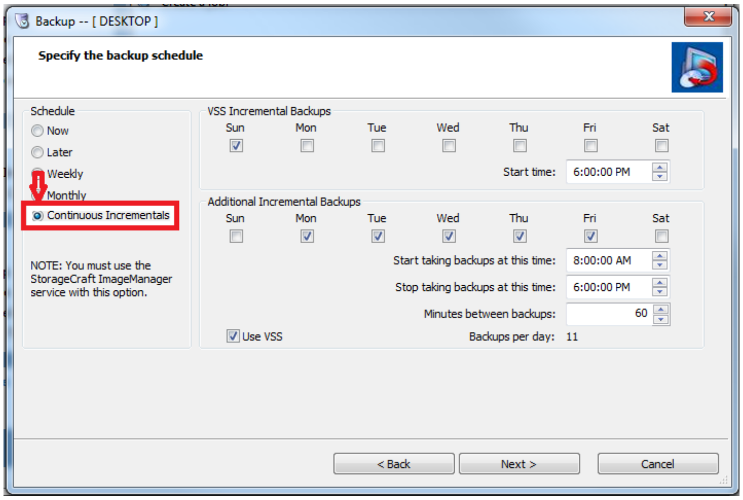
(\\192.168.1.20\VolumeImages\Server)

Specify image names

File Name	Volume
SYSTEM_VOL	*:\ (SYSTEM)
C_VOL	C:\ (OS)
D_VOL	D:\ (HP_RECOVERY)

* Double-click to rename file, or select it and hit space or F2

11. On the *Schedule* screen, select *Continuous Incrementals*. Set the desired schedule. The top row will run a single incremental backup. The bottom row will run multiple backups according to the set schedule.



Backup -- [DESKTOP]

Specify the backup schedule

Schedule
○ Now
○ Later
○ Weekly
○ Monthly
● Continuous Incrementals

NOTE: You must use the StorageCraft ImageManager service with this option.

VSS Incremental Backups

Sun	Mon	Tue	Wed	Thu	Fri	Sat
☑	☐	☐	☐	☐	☐	☐

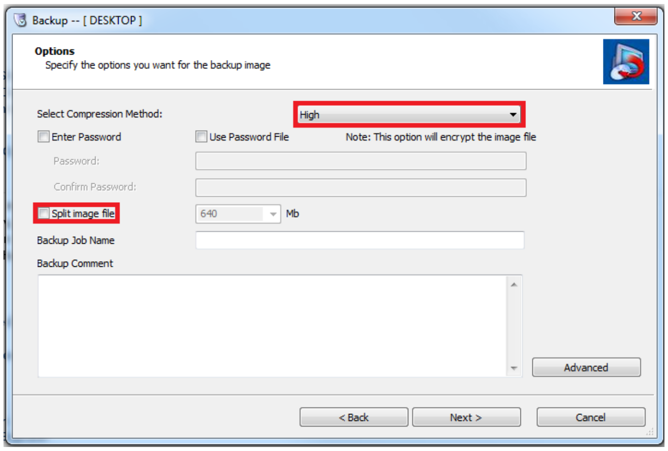
Start time: 6:00:00 PM

Additional Incremental Backups

Sun	Mon	Tue	Wed	Thu	Fri	Sat
☐	☑	☑	☑	☑	☑	☐

Start taking backups at this time: 8:00:00 AM
Stop taking backups at this time: 6:00:00 PM
Minutes between backups: 60
☑ Use VSS
Backups per day: 11

12. On the *Options* screen, we recommend that you select the *High* compression method. *High* has about a 50% compression while *Standard* has about a 40% compression. Do not split the image files.



Backup -- [DESKTOP]

Options
Specify the options you want for the backup image

Select Compression Method: High

☐ Enter Password ☐ Use Password File Note: This option will encrypt the image file

Password:

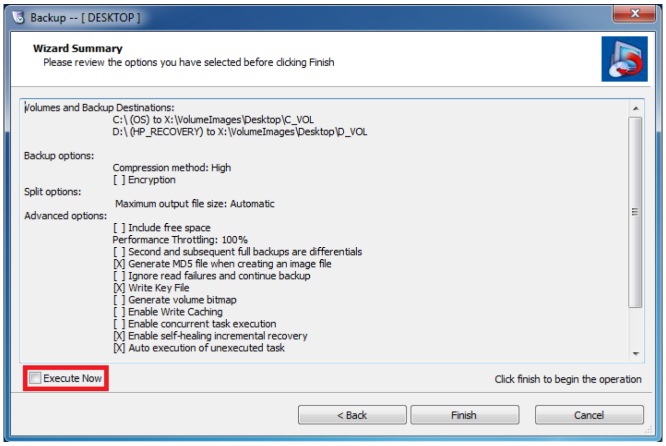
Confirm Password:

☐ Split image file 640 Mb

Backup Job Name

Backup Comment

13. On the *Wizard Summary* page, leave the Execute Now box uncheck to run the initial backup at the next scheduled time. If you wish to run the backup immediately, select the check box.



Backup -- [DESKTOP]

Wizard Summary
Please review the options you have selected before clicking Finish

```
Volumes and Backup Destinations:
                    C:\ (OS) to X:\VolumeImages\Desktop\C_VOL
                    D:\ (HP_RECOVERY) to X:\VolumeImages\Desktop\D_VOL

Backup options:
                    Compression method: High
                    [ ] Encryption
Split options:
                     Maximum output file size: Automatic
Advanced options:
                    [ ] Include free space
                    Performance Throttling: 100%
                    [ ] Second and subsequent full backups are differentials
                    [X] Generate MD5 file when creating an image file
                    [ ] Ignore read failures and continue backup
                    [X] Write Key File
                    [ ] Generate volume bitmap
                    [ ] Enable Write Caching
                    [ ] Enable concurrent task execution
                    [X] Enable self-healing incremental recovery
                    [X] Auto execution of unexecuted task
```

☐ Execute Now

Click finish to begin the operation

Configuring ImageManager

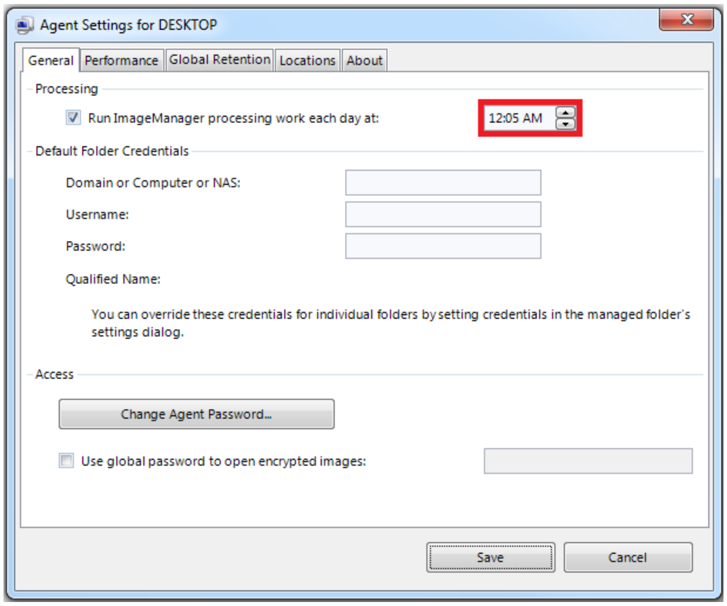
ShadowProtect uses forward deltas that require periodic management. ImageManager is a utility that consolidates hourly incrementals into daily incrementals, daily incrementals into weekly incrementals, weekly incrementals into monthly incrementals, and monthly incrementals into rolling incrementals. You 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 backup only the *daily*, *monthly*, and *rolling* collapsed incrementals. The hourly and weekly incrementals will not be backed up remotely.

1. The first step after installing ImageManager is to configure the settings. Click the ImageManager icon on the desktop.

2. Click the Agent Settings... near the bottom left corner.

3. Verify that ImageManager is set to run shortly after midnight, such as *12:05 A.M.*



Agent Settings for DESKTOP

Processing

☑ Run ImageManager processing work each day at: 12:05 AM

Default Folder Credentials

Domain or Computer or NAS:

Username:

Password:

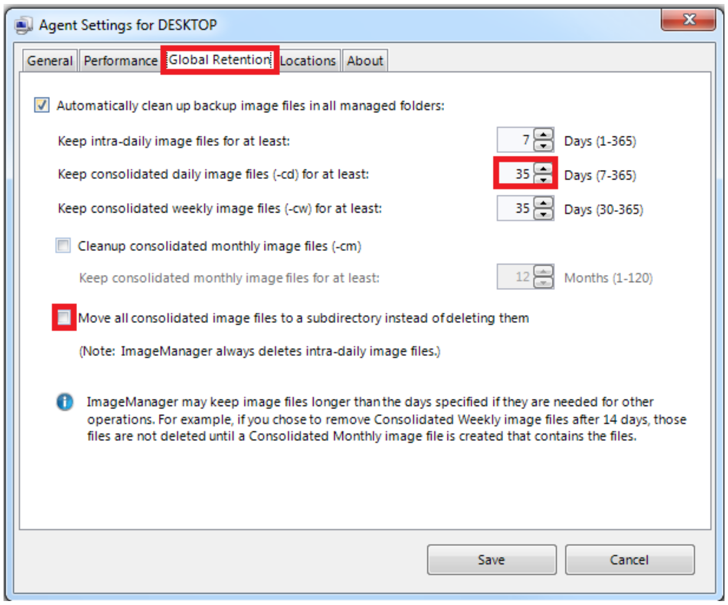
Qualified Name:

You can override these credentials for individual folders by setting credentials in the managed folder's settings dialog.

Access

☐ Use global password to open encrypted images:

4. Click the Global Retention tab. Verify that *Keep consolidated daily* is set to at least 35 days. Clear the last check box to *Move all consolidated image files to a subdirectory instead of deleting them.*



Agent Settings for DESKTOP

☑ Automatically clean up backup image files in all managed folders:

Keep intra-daily image files for at least: 7 Days (1-365)

Keep consolidated daily image files (-cd) for at least: 35 Days (7-365)

Keep consolidated weekly image files (-cw) for at least: 35 Days (30-365)

☐ Cleanup consolidated monthly image files (-cm)

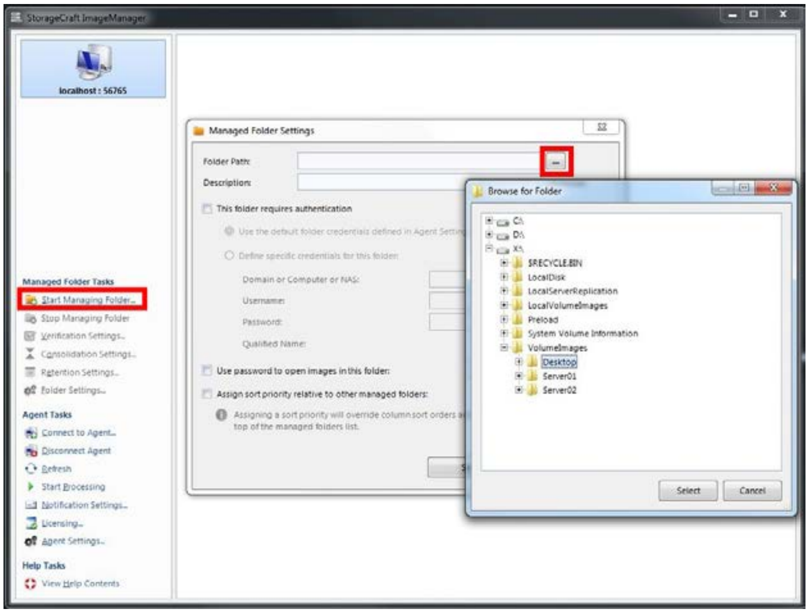
Keep consolidated monthly image files for at least: 12 Months (1-120)

☐ Move all consolidated image files to a subdirectory instead of deleting them

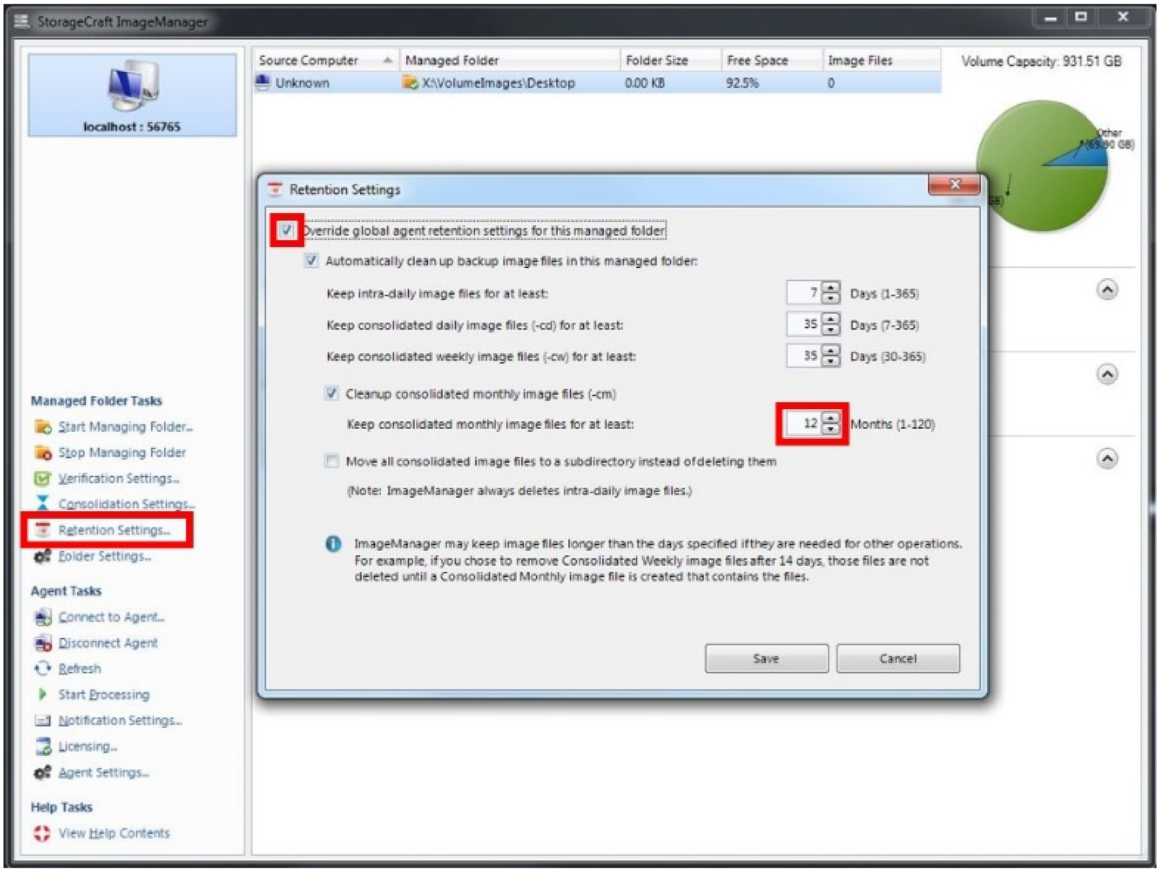
(Note: ImageManager always deletes intra-daily image files.)

ImageManager may keep image files longer than the days specified if they are needed for other operations. For example, if you chose to remove Consolidated Weekly image files after 14 days, those files are not deleted until a Consolidated Monthly image file is created that contains the files.

5. Next, click Start Managing Folder and browse to the folder that contains the ShadowProtect image files that you want to manage. Repeat for each folder that you want to manage.



6. You can override the global retention settings by highlighting the folder, selecting Retention Settings on the left side, clicking the checkbox *Override global agent retention settings for this managed folder,* and changing the desired settings.



Source Computer	Managed Folder	Folder Size	Free Space	Image Files
Unknown	X:\VolumeImages\Desktop	0.00 KB	92.5%	0

Retention Settings

☑ Override global agent retention settings for this managed folder

☑ Automatically clean up backup image files in this managed folder:

Keep intra-daily image files for at least: 7 Days (1-365)

Keep consolidated daily image files (-cd) for at least: 35 Days (7-365)

Keep consolidated weekly image files (-cw) for at least: 35 Days (30-365)

☑ Cleanup consolidated monthly image files (-cm)

Keep consolidated monthly image files for at least: 12 Months (1-120)

□ Move all consolidated image files to a subdirectory instead of deleting them

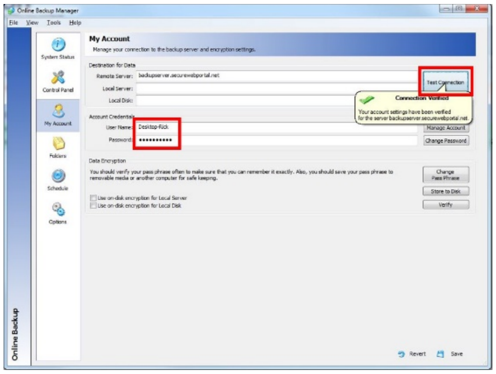
(Note: ImageManager always deletes intra-daily image files.)

ImageManager may keep image files longer than the days specified if they are needed for other operations. For example, if you chose to remove Consolidated Weekly image files after 14 days, those files are not deleted until a Consolidated Monthly image file is created that contains the files.

Configuring eFolder Online Backup Manager

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

2. Select the My Account tab. Enter the *User Name* and *Password* for the eFolder account and click the Test Connection button on the top right. Contact Technical Support if the *Connection Verified* window does *not* appear.



My Account

Manage your connection to the backup server and encryption settings.

Destination for Data

Remote Server: backupserver.securewebportal.net

Local Server:

Local Disk:

Connection Verified

Your account settings have been verified for the server backupserver.securewebportal.net.

Account Credentials

User Name: Desktop-Rick

Password: ••••••••••

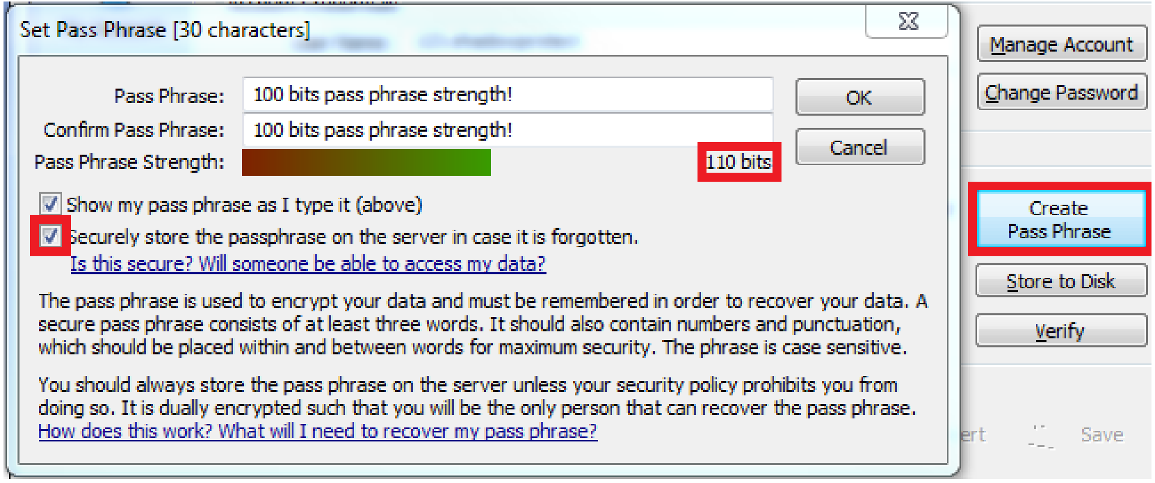
Data Encryption

You should verify your pass phrase often to make sure that you can remember it exactly. Also, you should save your pass phrase to removable media or another computer for safe keeping.

☐ Use on-disk encryption for Local Server

☐ Use on-disk encryption for Local Disk

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



Set Pass Phrase [30 characters]

Pass Phrase: 100 bits pass phrase strength!

Confirm Pass Phrase: 100 bits pass phrase strength!

Pass Phrase Strength: 110 bits

☑ Show my pass phrase as I type it (above)

☑ Securely store the passphrase on the server in case it is forgotten.

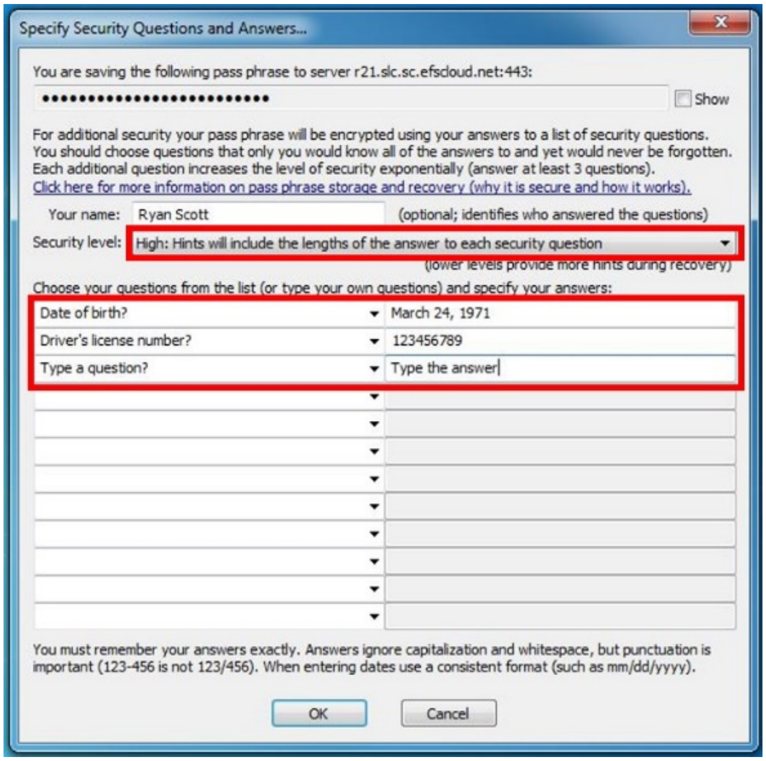
Is this secure? Will someone be able to access my data?

The pass phrase is used to encrypt your data and must be remembered in order to recover your data. A secure pass phrase consists of at least three words. It should also contain numbers and punctuation, which should be placed within and between words for maximum security. The phrase is case sensitive.

You should always store the pass phrase on the server unless your security policy prohibits you from doing so. It is dually encrypted such that you will be the only person that can recover the pass phrase.

How does this work? What will I need to recover my pass phrase?

4. To store the Pass Phrase in the eFolder Cloud, create a least three questions and answers. You can use the predefined questions or create your own. Set the desired security level.



Specify Security Questions and Answers...

You are saving the following pass phrase to server r21.slc.sc.efscloud.net:443:

•••••••••••••••••••••••••• □ Show

For additional security your pass phrase will be encrypted using your answers to a list of security questions. You should choose questions that only you would know all of the answers to and yet would never be forgotten. Each additional question increases the level of security exponentially (answer at least 3 questions).

Click here for more information on pass phrase storage and recovery (why it is secure and how it works).

Your name: Ryan Scott (optional; identifies who answered the questions)

Security level: High: Hints will include the lengths of the answer to each security question

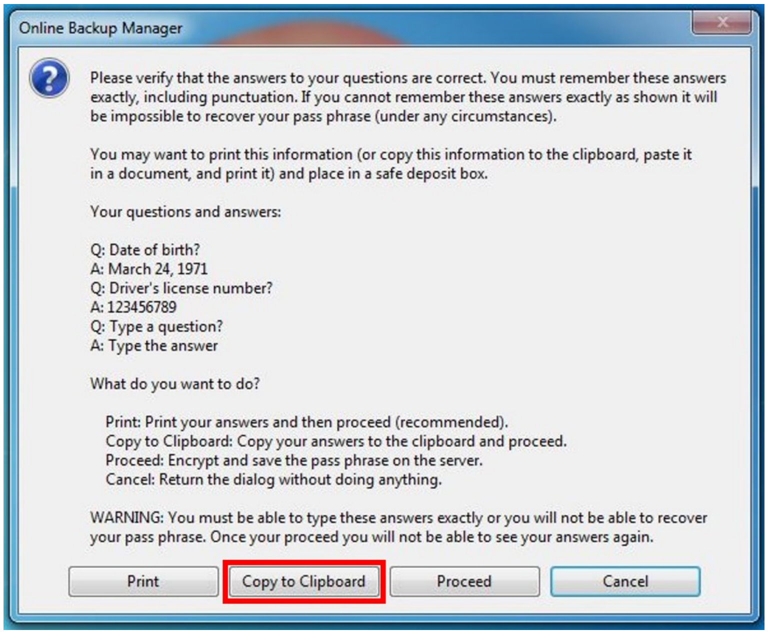
(lower levels provide more hints during recovery)

Choose your questions from the list (or type your own questions) and specify your answers:

Date of birth?	March 24, 1971
Driver's license number?	123456789
Type a question?	Type the answer

You must remember your answers exactly. Answers ignore capitalization and whitespace, but punctuation is important (123-456 is not 123/456). When entering dates use a consistent format (such as mm/dd/yyyy).

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.



Online Backup Manager

Please verify that the answers to your questions are correct. You must remember these answers exactly, including punctuation. If you cannot remember these answers exactly as shown it will be impossible to recover your pass phrase (under any circumstances).

You may want to print this information (or copy this information to the clipboard, paste it in a document, and print it) and place in a safe deposit box.

Your questions and answers:

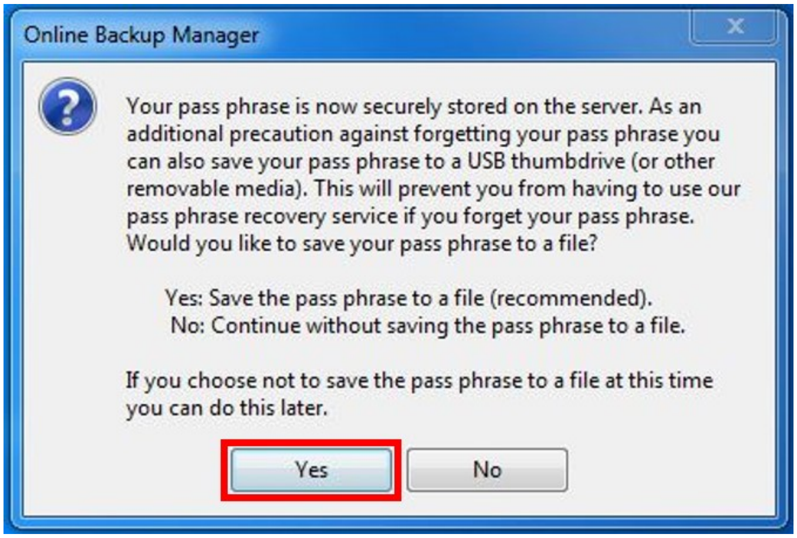
Q: Date of birth?
A: March 24, 1971
Q: Driver's license number?
A: 123456789
Q: Type a question?
A: Type the answer

What do you want to do?

Print: Print your answers and then proceed (recommended).
Copy to Clipboard: Copy your answers to the clipboard and proceed.
Proceed: Encrypt and save the pass phrase on the server.
Cancel: Return the dialog without doing anything.

WARNING: You must be able to type these answers exactly or you will not be able to recover your pass phrase. Once your proceed you will not be able to see your answers again.

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



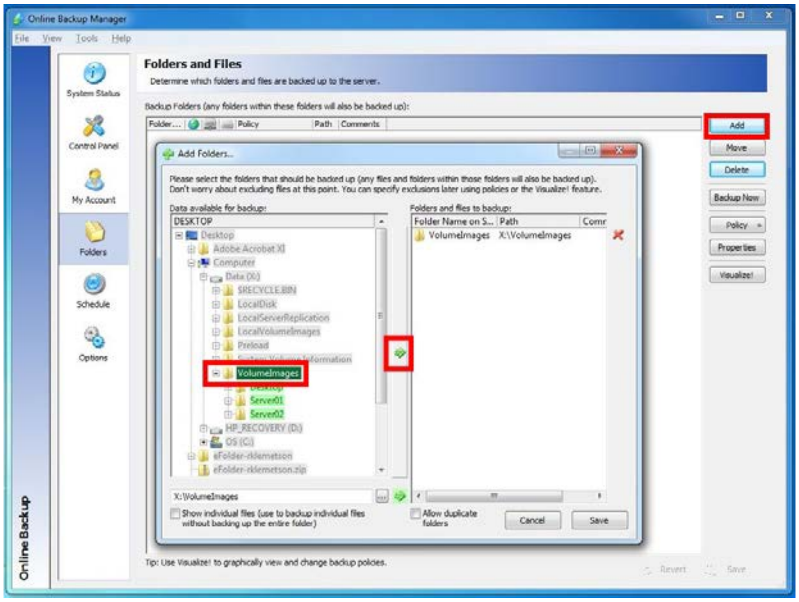
Online Backup Manager

Your pass phrase is now securely stored on the server. As an additional precaution against forgetting your pass phrase you can also save your pass phrase to a USB thumbdrive (or other removable media). This will prevent you from having to use our pass phrase recovery service if you forget your pass phrase. Would you like to save your pass phrase to a file?

Yes: Save the pass phrase to a file (recommended).
No: Continue without saving the pass phrase to a file.

If you choose not to save the pass phrase to a file at this time you can do this later.

7. To add the *VolumeImages* folder to the folders that will be backed up, click the Folders button, click Add, browse to the *X:\VolumeImages* folder, click the green arrow to move it to the right side of the screen, and then click Save.



Online Backup Manager

Folders and Files

Determine which folders and files are backed up to the server.

Backup Folders (any folders within these folders will also be backed up):

Add Folders...

Please select the folders that should be backed up (any files and folders within those folders will also be backed up). Don't worry about excluding files at this point. You can specify exclusions later using policies or the Visualize! feature.

Data available for backup:

```
DESKTOP
⊟ Desktop
  ⊞ Adobe Acrobat XI
  ⊟ Computer
    ⊟ Data (X:)
      ⊞ $RECYCLE.BIN
      ⊞ LocalDisk
      ⊞ LocalServerReplication
      ⊞ LocalVolumeImages
      ⊞ Preload
      ⊞ System Volume Information
      ⊟ VolumeImages
        ⊞ Desktop
        ⊞ Server01
        ⊞ Server02
    ⊞ HP_RECOVERY (D:)
    ⊞ OS (C:)
  ⊞ eFolder-rklemetson
  eFolder-rklemetson.zip
```

X:\VolumeImages

□ Show individual files (use to backup individual files without backing up the entire folder)

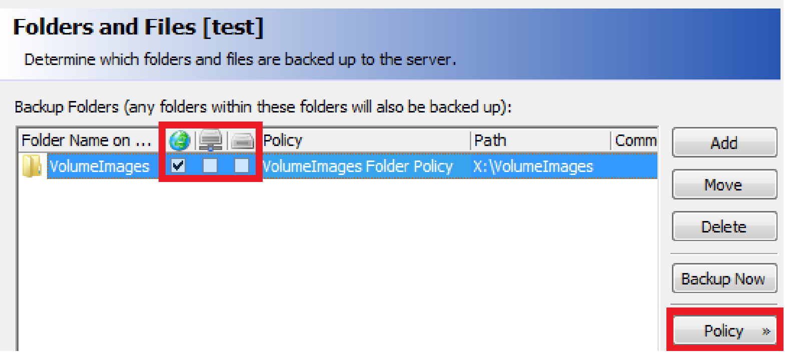
Folders and files to backup:

Folder Name on S...	Path	Comr
VolumeImages	X:\VolumeImages	

□ Allow duplicate folders

Tip: Use Visualize! to graphically view and change backup policies.

8. Clear the checkboxes for the columns that are *not* configured for backups. The three columns are Cloud Backup, Local Server, Local Disk. Highlight the *VolumeImages* folder, click Policy on the right side, select Edit Policy.



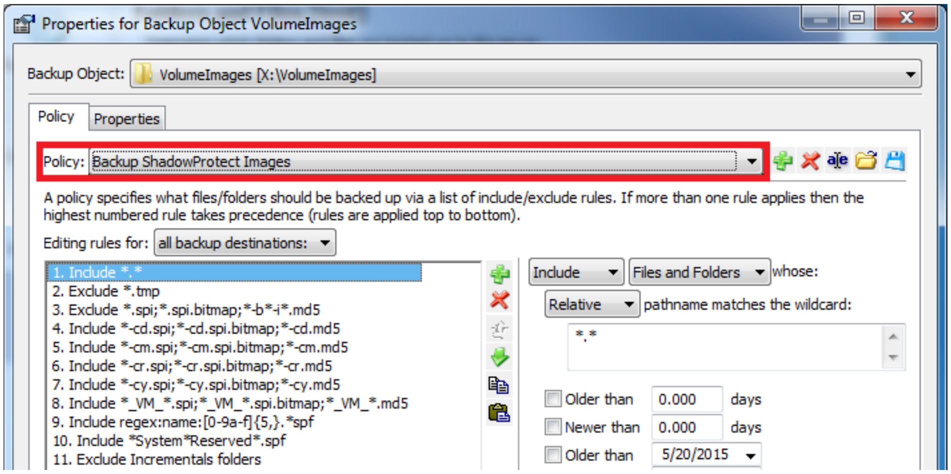
Folders and Files [test]

Determine which folders and files are backed up to the server.

Backup Folders (any folders within these folders will also be backed up):

Folder Name on ...				Policy	Path	Comm
VolumeImages	☑	□	□	VolumeImages Folder Policy	X:\VolumeImages	

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



Properties for Backup Object VolumeImages

Backup Object: VolumeImages [X:\VolumeImages]

Policy | Properties

Policy: Backup ShadowProtect Images

A policy specifies what files/folders should be backed up via a list of include/exclude rules. If more than one rule applies then the highest numbered rule takes precedence (rules are applied top to bottom).

Editing rules for: all backup destinations:

1. Include *.*
2. Exclude *.tmp
3. Exclude *.spi;*.spi.bitmap;*-b*-i*.md5
4. Include *-cd.spi;*-cd.spi.bitmap;*-cd.md5
5. Include *-cm.spi;*-cm.spi.bitmap;*-cm.md5
6. Include *-cr.spi;*-cr.spi.bitmap;*-cr.md5
7. Include *-cy.spi;*-cy.spi.bitmap;*-cy.md5
8. Include *_VM_*.spi;*_VM_*.spi.bitmap;*_VM_*.md5
9. Include regex:name:[0-9a-f]{5,}.*spf
10. Include *System*Reserved*.spf
11. Exclude Incrementals folders

Include | Files and Folders whose:

Relative pathname matches the wildcard:

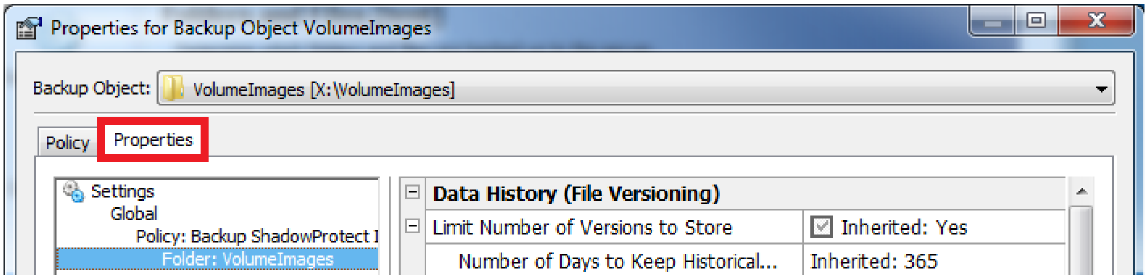
.

□ Older than 0.000 days

□ Newer than 0.000 days

□ Older than 5/20/2015

10. Click the Properties tab.



Properties for Backup Object VolumeImages

Backup Object: VolumeImages [X:\VolumeImages]

Policy | Properties

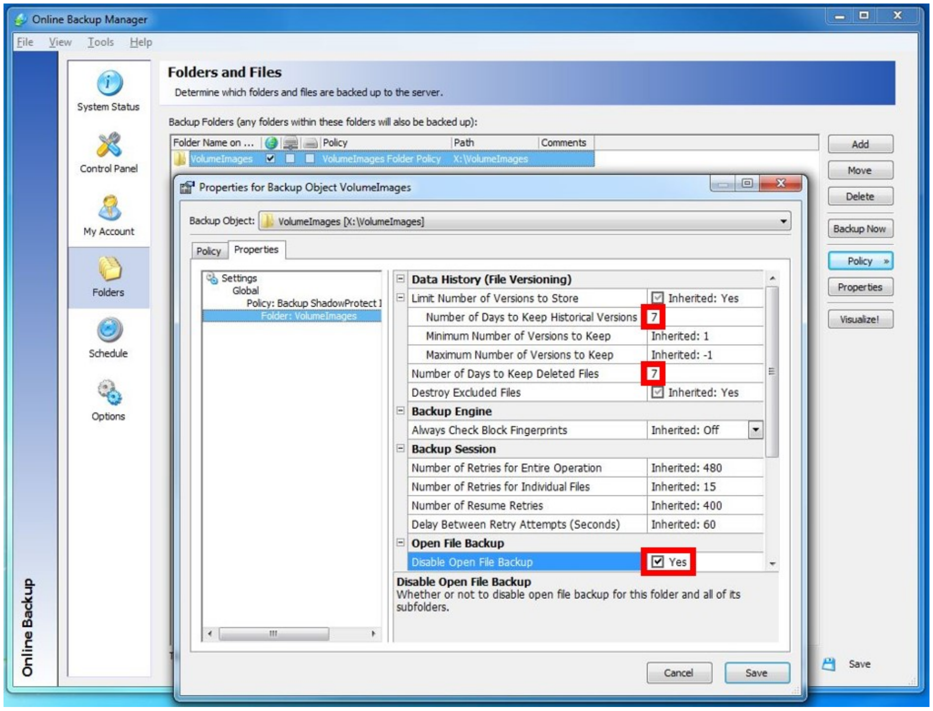
Settings
Global
Policy: Backup ShadowProtect I
Folder: VolumeImages

Data History (File Versioning)

Limit Number of Versions to Store ☑ Inherited: Yes

Number of Days to Keep Historical... Inherited: 365

11. On the *Properties* tab, 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.* Change *Disable Open File Backup* to *Yes*.



Folders and Files

Determine which folders and files are backed up to the server.

Backup Folders (any folders within these folders will also be backed up):

Folder Name on ...				Policy	Path	Comments
VolumeImages	☑	□	□	VolumeImages Folder Policy	X:\VolumeImages	

Properties for Backup Object VolumeImages

Backup Object: VolumeImages [X:\VolumeImages]

Policy | Properties

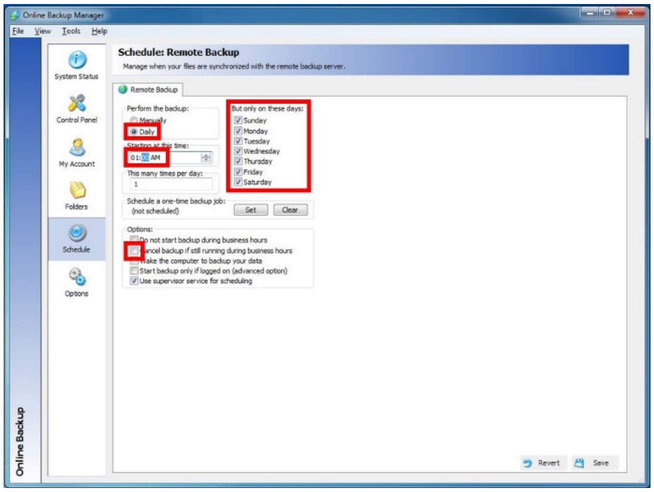
Settings
Global
Policy: Backup ShadowProtect I
Folder: VolumeImages

Data History (File Versioning)	
Limit Number of Versions to Store	☑ Inherited: Yes
Number of Days to Keep Historical Versions	7
Minimum Number of Versions to Keep	Inherited: 1
Maximum Number of Versions to Keep	Inherited: -1
Number of Days to Keep Deleted Files	7
Destroy Excluded Files	☑ Inherited: Yes
Backup Engine	
Always Check Block Fingerprints	Inherited: Off
Backup Session	
Number of Retries for Entire Operation	Inherited: 480
Number of Retries for Individual Files	Inherited: 15
Number of Resume Retries	Inherited: 400
Delay Between Retry Attempts (Seconds)	Inherited: 60
Open File Backup	
Disable Open File Backup	☑ Yes

Disable Open File Backup
Whether or not to disable open file backup for this folder and all of its subfolders.

Cancel Save

12. Click the Schedule tab on the left. Verify that *Daily* is selected. Set the time to about *1:00 AM* and verify that all seven days are selected. Verify that the checkbox *Cancel backup if still running during business hours* is cleared.



Schedule: Remote Backup

Manage when your files are synchronized with the remote backup server.

Perform the backup:
○ Manually
● Daily

Starting at this time: 01:00 AM

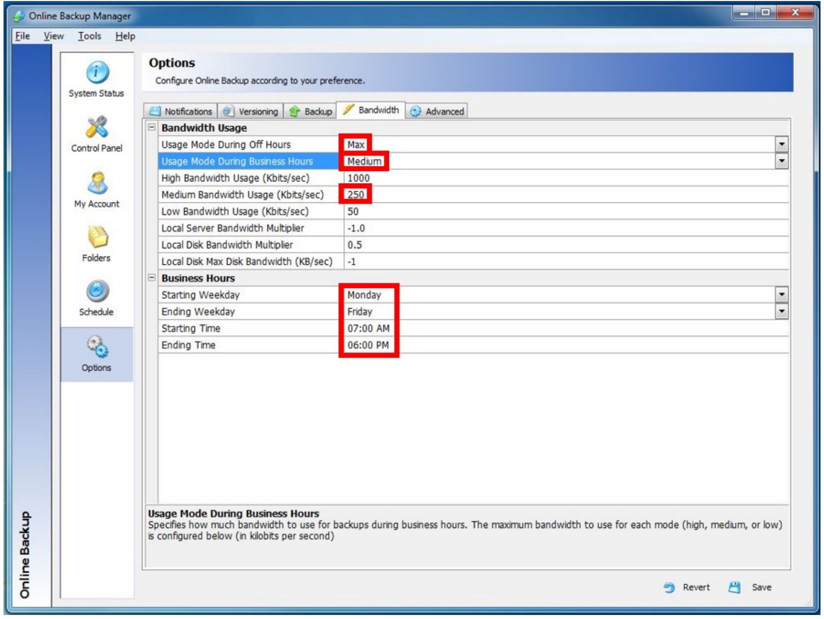
This many times per day: 1

But only on these days:
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Schedule a one-time backup job: (not scheduled)

Options:
□ Do not start backup during business hours
□ Cancel backup if still running during business hours
□ Wake the computer to backup your data
□ Start backup only if logged on (advanced option)
☑ Use supervisor service for scheduling

13. Click the Options tab on the left. Then click the Bandwidth tab at the top.
14. Set the *Business Hours* to an hour before and after the employees' normal working hours.
15. Set the *Usage Mode During Business Hours* field to *Medium* and then set *Medium Bandwidth Usage* field to *25% of the customer's upload speed.*
16. Set the *Usage Mode During Off Hours* field to *Max*. If the client needs the Internet afterhours, set this field to *High* and then set the *High Bandwidth Usage* field to *75% of the customer's upload speed.*



Options

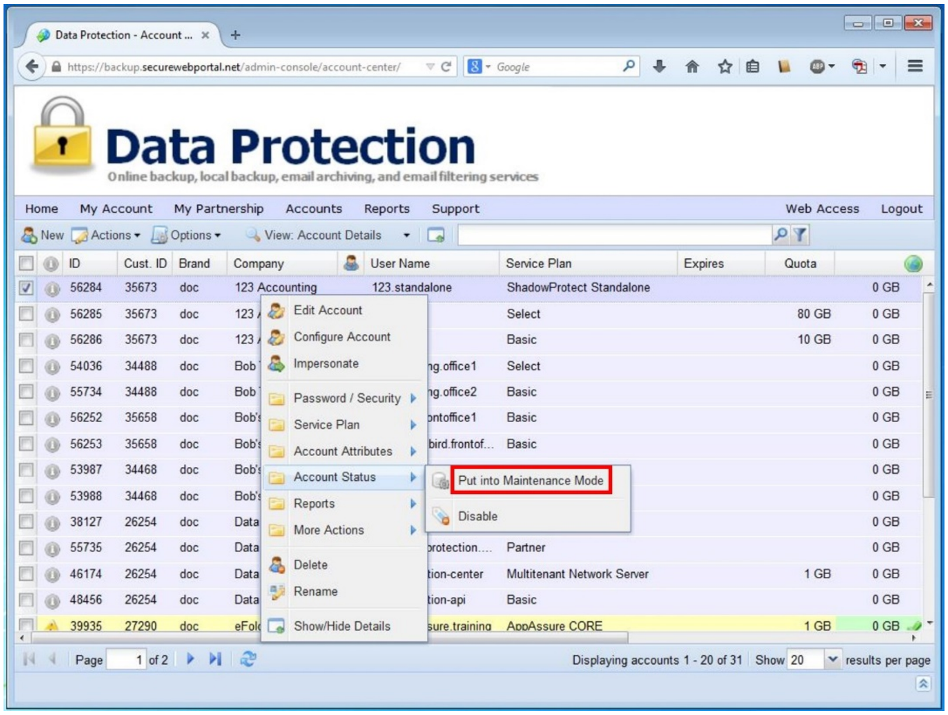
Configure Online Backup according to your preference.

Bandwidth Usage	
Usage Mode During Off Hours	Max
Usage Mode During Business Hours	Medium
High Bandwidth Usage (Kbits/sec)	1000
Medium Bandwidth Usage (Kbits/sec)	250
Low Bandwidth Usage (Kbits/sec)	50
Local Server Bandwidth Multiplier	-1.0
Local Disk Bandwidth Multiplier	0.5
Local Disk Max Disk Bandwidth (KB/sec)	-1
Business Hours	
Starting Weekday	Monday
Ending Weekday	Friday
Starting Time	07:00 AM
Ending Time	06:00 PM

Usage Mode During Business Hours

Specifies how much bandwidth to use for backups during business hours. The maximum bandwidth to use for each mode (high, medium, or low) is configured below (in kilobits per second)

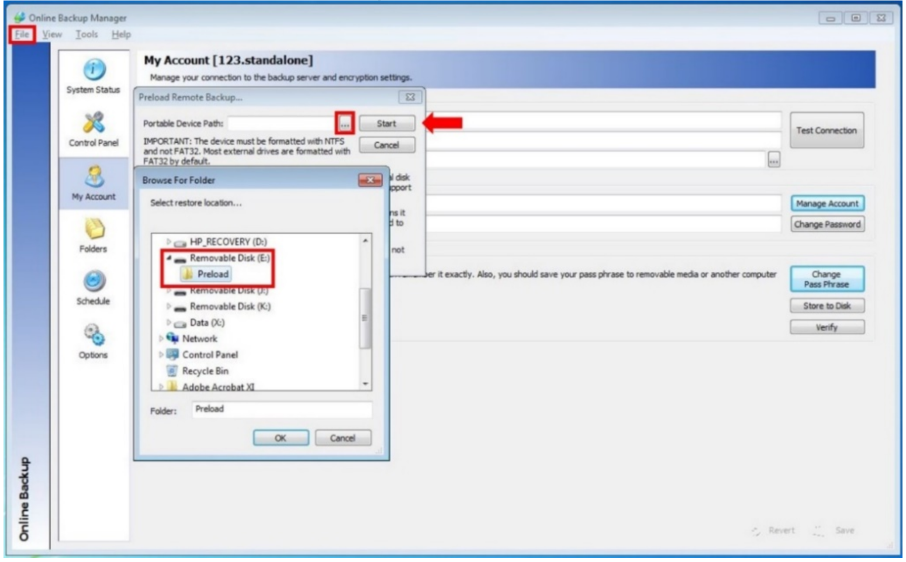
17. If you want to create a preload drive or seeding drive to ship to the eFolder data center, first put the account into maintenance mode by selecting *Account Center* in the Accounts main menu bar of the eFolder Web Portal, right-clicking the desired account, and selecting *Put into Maintenance Mode* in the Account Status menu option.



	ID	Cust. ID	Brand	Company	User Name	Service Plan	Expires	Quota	
☑	56284	35673	doc	123 Accounting	123.standalone	ShadowProtect Standalone			0 GB
□	56285	35673	doc	123		Select		80 GB	0 GB
□	56286	35673	doc	123		Basic		10 GB	0 GB
□	54036	34488	doc	Bob	ng.office1	Select			0 GB
□	55734	34488	doc	Bob	ng.office2	Basic			0 GB
□	56252	35658	doc	Bob's	ontoffice1	Basic			0 GB
□	56253	35658	doc	Bob's	bird.frontof...	Basic			0 GB
□	53987	34468	doc	Bob's					0 GB
□	53988	34468	doc	Bob's					0 GB
□	38127	26254	doc	Data					0 GB
□	55735	26254	doc	Data	protection....	Partner			0 GB
□	46174	26254	doc	Data	tion-center	Multitenant Network Server		1 GB	0 GB
□	48456	26254	doc	Data	tion-api	Basic			0 GB
□	39935	27290	doc	eFol	sure.training	AppAssure CORE		1 GB	0 GB

Page 1 of 2 Displaying accounts 1 - 20 of 31 Show 20 results per page

18. Next, perform the initial Preload backup to the USB disk. To do this, open the Backup Manager, click File on the menu bar, and select *Preload Remote Backup*. Then specify a new empty directory on the external USB disk. When you are ready, click the Start button.
Note: You can run Preload multiple times before shipping the drive to the data center. It will copy new and additional files that were not copied previously. Once the data center team loads, the data to the cloud servers, then will take the account out of maintenance mode and the backups will run as scheduled.



My Account [123.standalone]
Manage your connection to the backup server and encryption settings.

Preload Remote Backup...
Portable Device Path:
IMPORTANT: The device must be formatted with NTFS and not FAT32. Most external drives are formatted with FAT32 by default.

Browse For Folder
Select restore location...
- HP_RECOVERY (D:)
- Removable Disk (E:)
  - Preload
- Removable Disk (J:)
- Removable Disk (K:)
- Data (X:)
- Network
- Control Panel
- Recycle Bin
- Adobe Acrobat XI

Folder: Preload

...er it exactly. Also, you should save your pass phrase to removable media or another computer

⚠ CAUTION: Never destroy any of the full backup or incremental files (*.spf, *.spi) in the backup repository. ShadowProtect continuous backups require an unbroken chain of deltas back to the full backup in order to restore a current volume image properly. Older daily delta files will be automatically purged from the backup when it is safe to do so according to the retention settings as described above.

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. See the eFolder Continuity Cloud ShadowProtect Howto Guide 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.

You should make sure that you are utilizing the notification and alerting features in the eFolder partner 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 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.

TIP: 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 to restore any remaining file-based data as needed.
6. With all data fully restored, set the eFolder schedule back to Weekly.

Additional Assistance

We will assist you any way that we can. Please submit questions to support@efolder.net, call us at 800-352-0248, or browse our knowledge base at https://secure.efoldering.com/support/kb/