Purpose

The purpose of this knowledgebase article is to help you back up your data files for safe keeping OR to send to White Light Computing during an extensive support incident. Please read the entire article before proceeding.

Please note: White Light Computing treats your data with confidentiality and takes precautions with your information to the best of their abilities. If you are uncomfortable with transferring your data to White Light Computing please let us know. You can also password protect the data using tools like WinZIP, 7ZIP, and other compression tools, but this is outside the scope of this article.

DISCLAIMER: This information is provided "as is". The author, publishers and marketers of this information disclaim any loss or liability, either directly or indirectly as a consequence of applying the information presented herein, or in regard to the use and application of said information. No guarantee is given, either expressed or implied, in regard to the merchantability, accuracy, or acceptability of the information.

General Recommendations

White Light Computing **strongly** encourages our customers to back up their data as often as practical, and definitely once-a-day if there are any changes to the data. The current version of SOS offers a complete backup of your SOS data.

Additionally, some customers have server backup and full workstation processes that run automatically on the computers where SOS is installed. These are perfectly good if they back up the SOS folder and all subfolders.

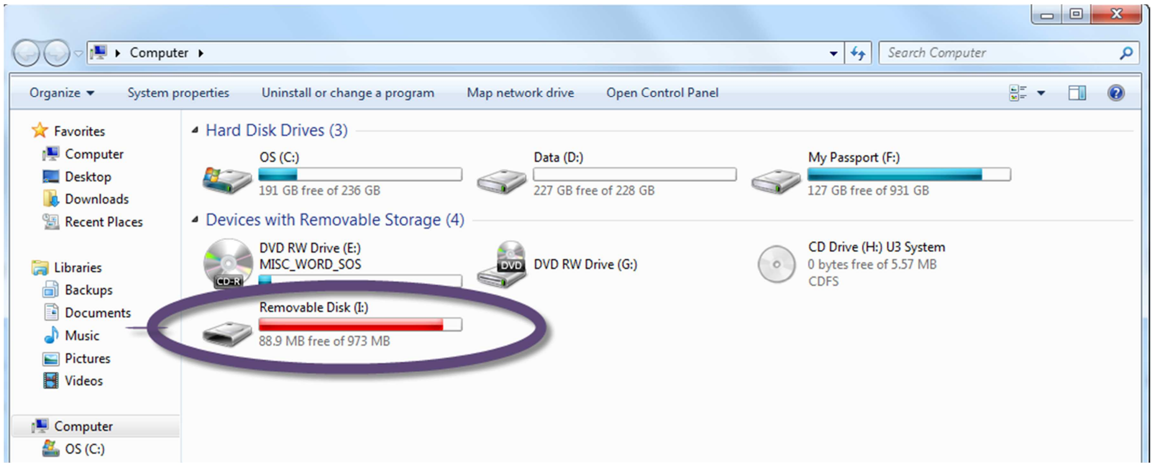
To be very clear, regardless of how backups are done no one should be running SOS during a backup process. All computers used to run SOS should have SOS shut down. We cannot ensure that good backups are made if anyone else has SOS open.

> **NOTE: We recommend taking the recent/current backups offsite from your location and leaving a copy of the latest backup at your office. It could be as simple as someone with authority to take it home, but we recommend something like a safety deposit box at a bank that is protected from fire and extreme weather. Something like a hurricane or tornado can easily hit both the home and office in one weather event.**
>
> **You also can consult with your IT support staff to see what recommendations they might have for offsite backups provided over the Internet. These services provide an additional layer of security where backups are not located in the same town. Typically there are charges for this type of service.**

Setup: Backing Up SOS on a USB Drive

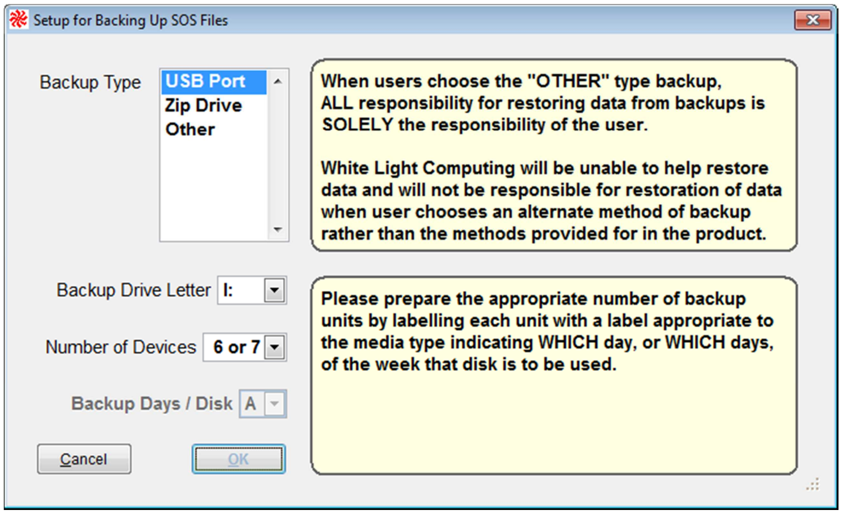
1) First, determine what “drive letter” your computer assigns to your USB drive:
   - QUIT out of SOS, so that you are looking at the Windows “desktop” screen
   - Insert a USB drive into one of your computer’s USB ‘ports’
   - Look for an icon labeled MY COMPUTER or COMPUTER and double-click on it
   - If there’s no such an icon, click START, double-click on an entry for MY COMPUTER or COMPUTER

   Below is an example of the COMPUTER window on one of our computers:



   - Your USB drive may appear labeled as “Removable Disk (I:)” as one of ours above is labeled.
   - Usually your USB drive will be E, F or G. Our machine just has more drives than most.
   - Write down the drive letter for your USB backup unit, then close the My Computer or Computer window.

2) Start SOS. Go to Management→ Setup Activities→ Backup Setup. You’ll see a window:



Backup Type: USB Port / Zip Drive / Other

When users choose the "OTHER" type backup, ALL responsibility for restoring data from backups is SOLELY the responsibility of the user.

White Light Computing will be unable to help restore data and will not be responsible for restoration of data when user chooses an alternate method of backup rather than the methods provided for in the product.

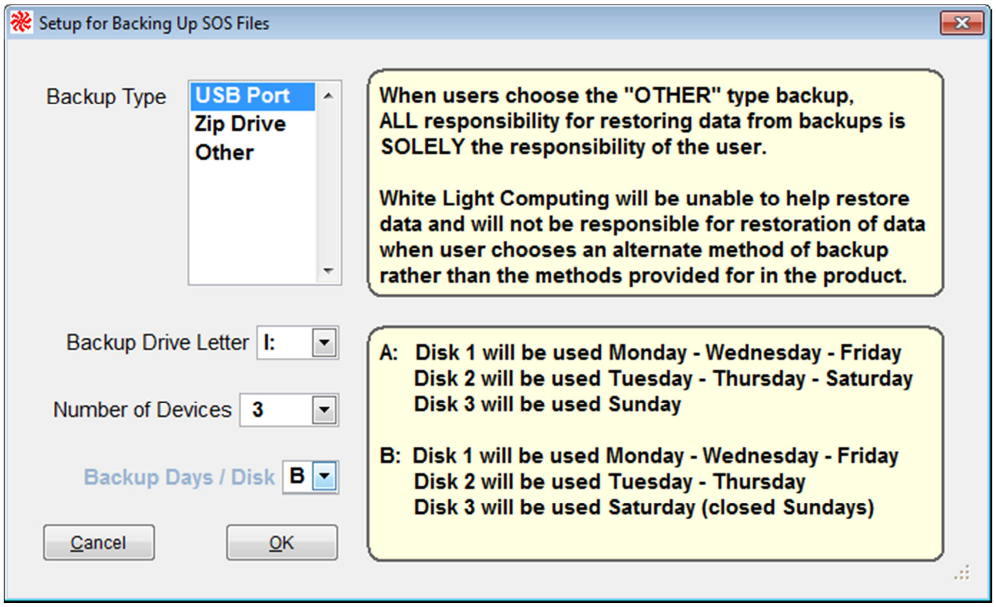
Backup Drive Letter: I:

Number of Devices: 6 or 7

Backup Days / Disk: A

Please prepare the appropriate number of backup units by labelling each unit with a label appropriate to the media type indicating WHICH day, or WHICH days, of the week that disk is to be used.

3) Answer the questions about your backup situation:
   - USB would be your selection for Backup Type
   - Backup Drive Letter is the letter you wrote down in step 2
   - Number of devices/disks is either:
     - 7—**RECOMMENDED**—One for each day of the week that you are open
     - 3—One for backups on Monday, Wednesday, and Friday, another for Tuesday and Thursday and Saturday, and a final one for Sunday (or Saturday if you are not open Sundays)



Backup Type: USB Port

When users choose the "OTHER" type backup, ALL responsibility for restoring data from backups is SOLELY the responsibility of the user.

White Light Computing will be unable to help restore data and will not be responsible for restoration of data when user chooses an alternate method of backup rather than the methods provided for in the product.

Backup Drive Letter: I:

Number of Devices: 3

Backup Days / Disk: B

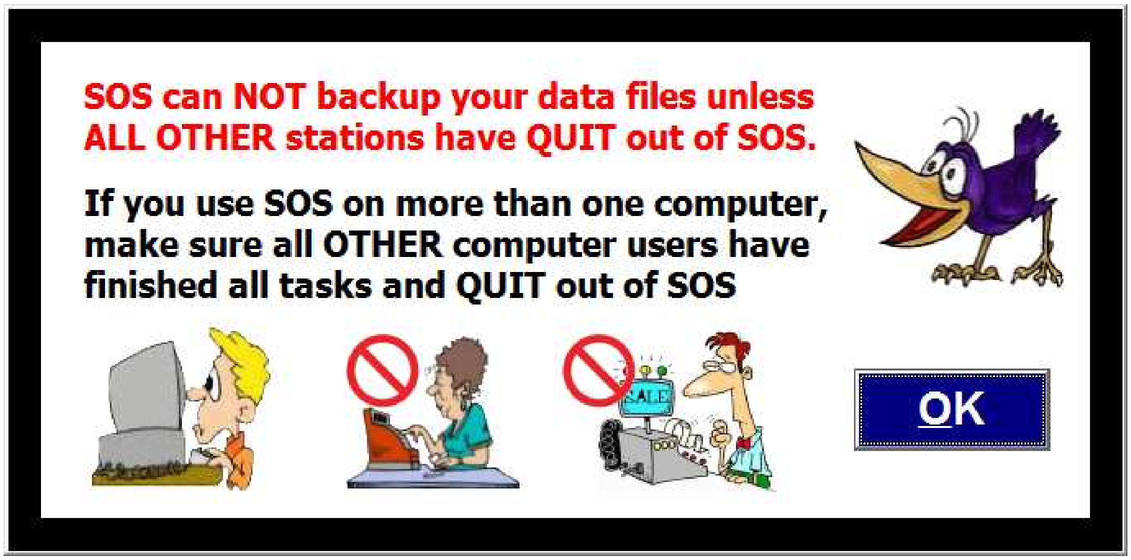
A: Disk 1 will be used Monday - Wednesday - Friday
Disk 2 will be used Tuesday - Thursday - Saturday
Disk 3 will be used Sunday

B: Disk 1 will be used Monday - Wednesday - Friday
Disk 2 will be used Tuesday - Thursday
Disk 3 will be used Saturday (closed Sundays)

   - Backup type is A if you're open 7 days a week (answer defaults if 7 is selected), otherwise B
   - Click OK to save your setup choices

How to Backup SOS EVERY Night

1) Make sure all other computers our out of SOS. When starting the backup process, this message will appear to remind you:

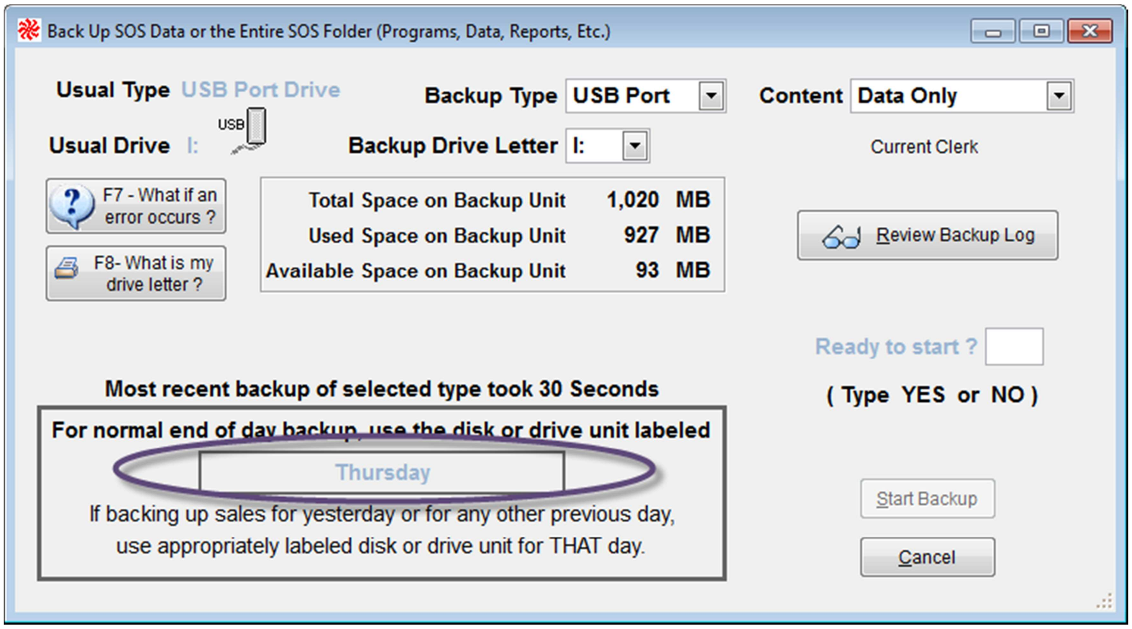


SOS can NOT backup your data files unless ALL OTHER stations have QUIT out of SOS.

If you use SOS on more than one computer, make sure all OTHER computer users have finished all tasks and QUIT out of SOS

2) Go END OF DAY, and select BACKUP.

NOTE: 6 or 7 USB drive backup setup will tell you which backup to use based on what day it is.



Back Up SOS Data or the Entire SOS Folder (Programs, Data, Reports, Etc.)

Usual Type USB Port Drive

Backup Type USB Port

Content Data Only

Usual Drive I:

Backup Drive Letter I:

Current Clerk

Total Space on Backup Unit	1,020	MB
Used Space on Backup Unit	927	MB
Available Space on Backup Unit	93	MB

Ready to start ?

(Type YES or NO)

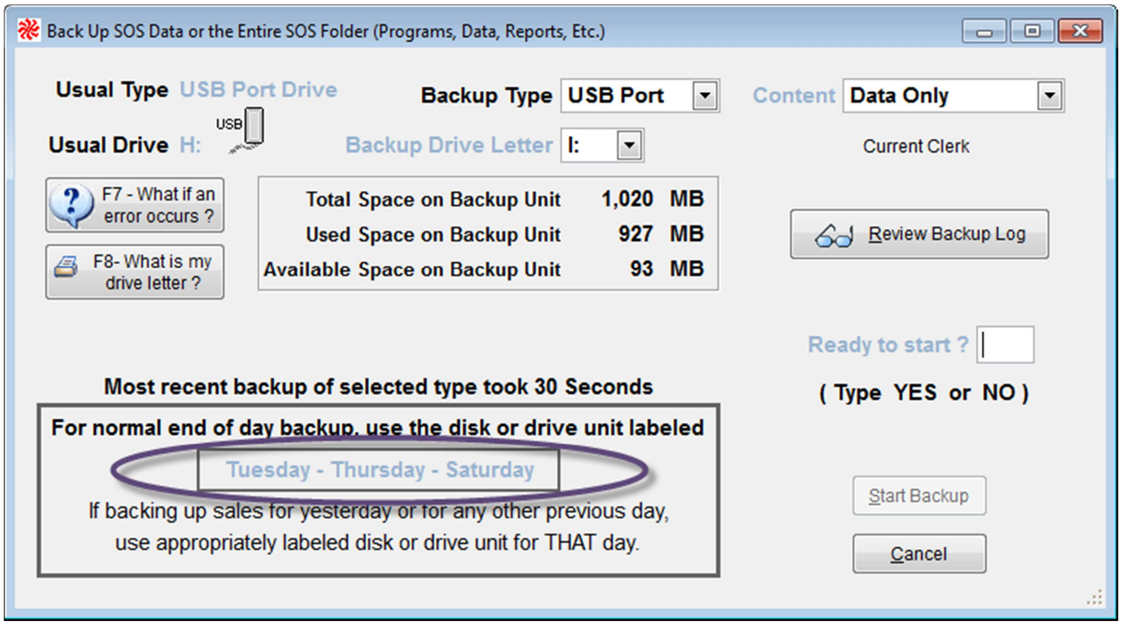
Most recent backup of selected type took 30 Seconds

For normal end of day backup, use the disk or drive unit labeled

Thursday

If backing up sales for yesterday or for any other previous day, use appropriately labeled disk or drive unit for THAT day.

NOTE: 3 USB drive backup setup will tell you which backup to use based on what day it is.


Back Up SOS Data or the Entire SOS Folder (Programs, Data, Reports, Etc.)

Usual Type USB Port Drive

Usual Drive H:

Backup Type USB Port

Backup Drive Letter I:

Content Data Only

Current Clerk

Total Space on Backup Unit	1,020	MB
Used Space on Backup Unit	927	MB
Available Space on Backup Unit	93	MB

Ready to start ?

(Type YES or NO)

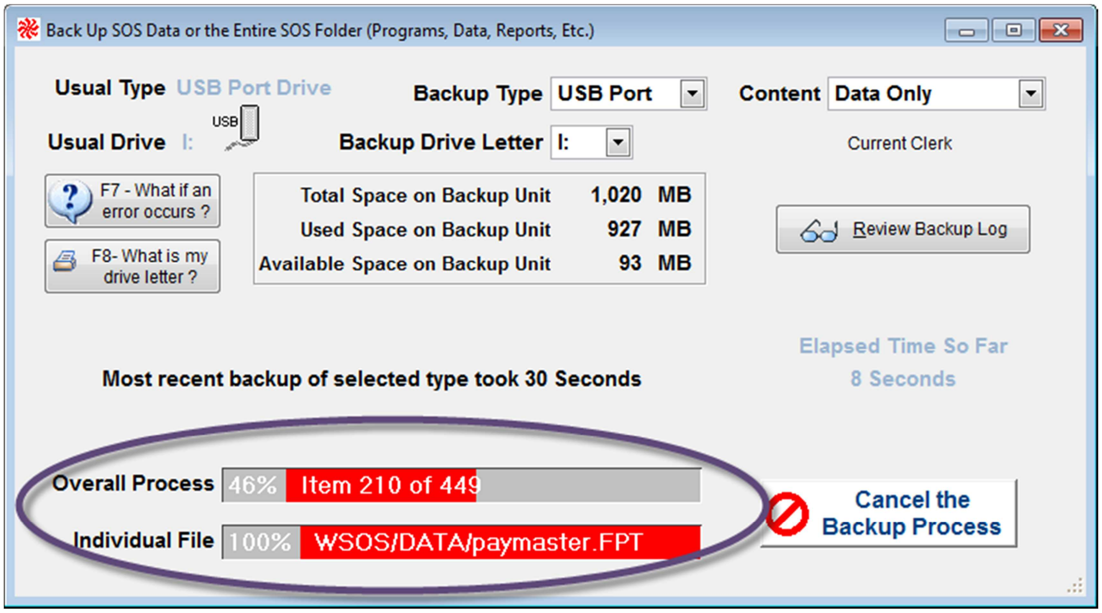
Most recent backup of selected type took 30 Seconds

For normal end of day backup, use the disk or drive unit labeled

Tuesday - Thursday - Saturday

If backing up sales for yesterday or for any other previous day, use appropriately labeled disk or drive unit for THAT day.

3) Review that your backup choices for backup type and backup drive letter are correct.
   - Choose the DATA ONLY option for CONTENT.
   - Type YES at the “Ready to start?” textbox.
   - Then watch the on-screen notes about backing up.
   - There’s a long pause at the beginning before the thermometer bar activates and displays backup status.


Back Up SOS Data or the Entire SOS Folder (Programs, Data, Reports, Etc.)

Usual Type USB Port Drive

Usual Drive I:

Backup Type USB Port

Backup Drive Letter I:

Content Data Only

Current Clerk

Total Space on Backup Unit	1,020	MB
Used Space on Backup Unit	927	MB
Available Space on Backup Unit	93	MB

Elapsed Time So Far
8 Seconds

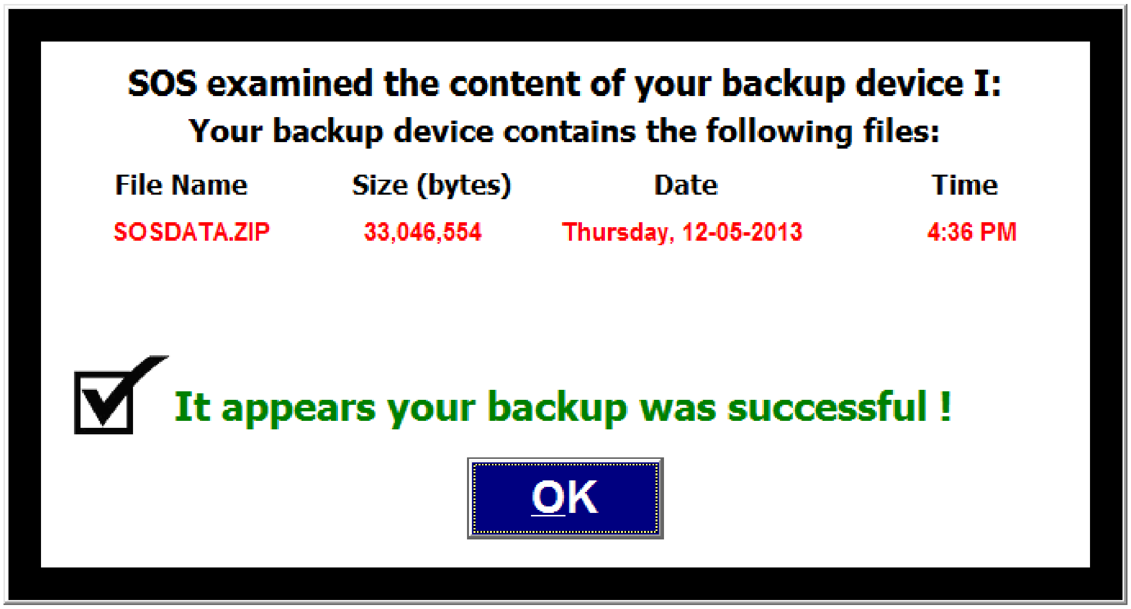
Most recent backup of selected type took 30 Seconds

Overall Process 46% Item 210 of 449

Individual File 100% WSOS/DATA/paymaster.FPT

USB
F7 - What if an error occurs ?
F8- What is my drive letter ?
Review Backup Log
Cancel the Backup Process

4) SOS will alert you when your backup was successful.

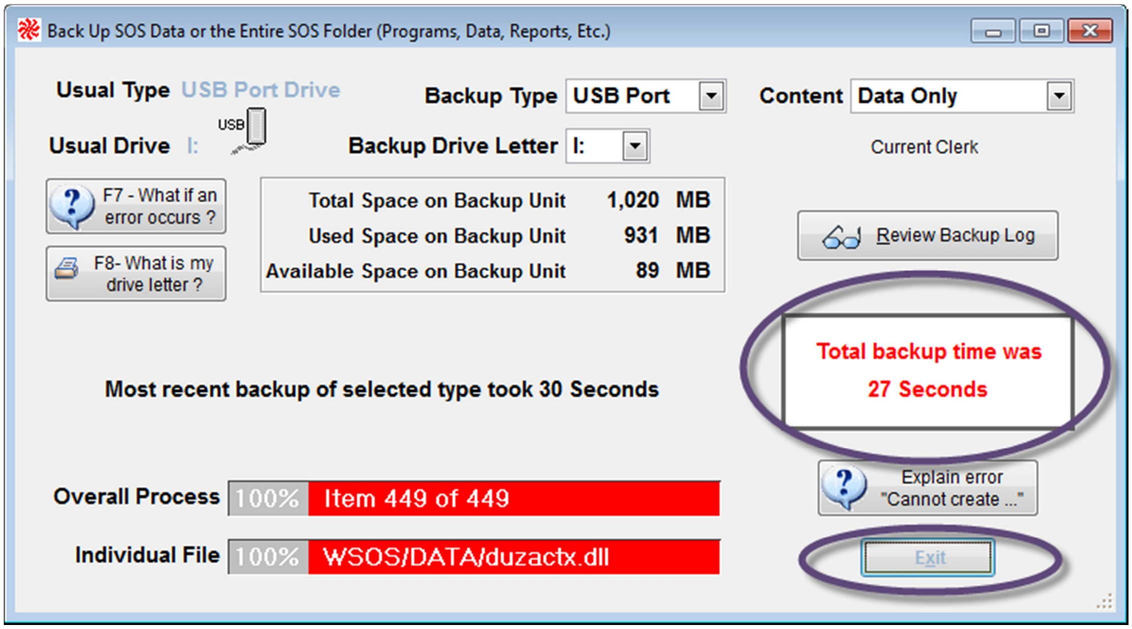


SOS examined the content of your backup device I:
Your backup device contains the following files:

File Name	Size (bytes)	Date	Time
SOSDATA.ZIP	33,046,554	Thursday, 12-05-2013	4:36 PM

☑ It appears your backup was successful !

5) SOS will tell you how long the backup took to complete. Click EXIT.



Back Up SOS Data or the Entire SOS Folder (Programs, Data, Reports, Etc.)

Usual Type USB Port Drive

Usual Drive I:

Backup Type USB Port

Backup Drive Letter I:

Content Data Only

Current Clerk

Total Space on Backup Unit	1,020	MB
Used Space on Backup Unit	931	MB
Available Space on Backup Unit	89	MB

Most recent backup of selected type took 30 Seconds

Total backup time was 27 Seconds

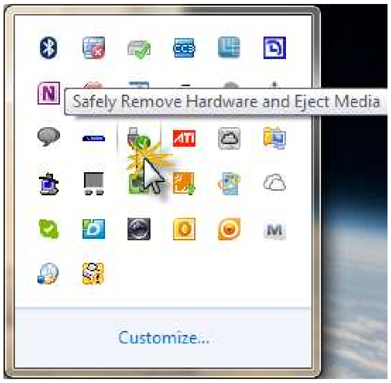
Overall Process 100% Item 449 of 449

Individual File 100% WSOS/DATA/duzactx.dll

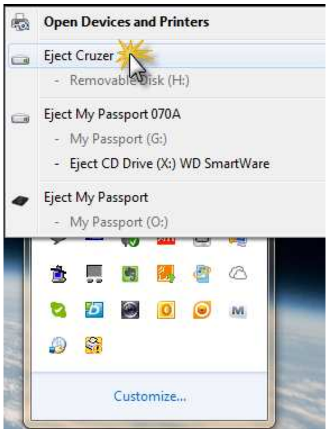
USB
F7 - What if an error occurs ?
F8- What is my drive letter ?
Review Backup Log
Explain error "Cannot create ..."
Exit

6) Once your backup is done you need to disconnect the USB device from your computer. You need to do this safely to ensure the integrity of the USB device. If you unplug an USB device or removable drive from your computer while it's transferring or saving information, you might risk losing some information. Windows provides a way to help you safely remove such devices.

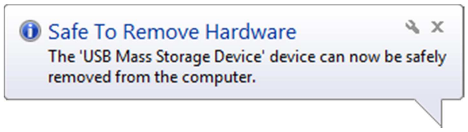
In the Windows notification area (lower right corner of task bar) you will find the icon to **Safely Remove Hardware**. The icon has a check mark in a green circle next to a computer. If you don't see the Safely Remove Hardware icon, click the Show hidden icons button to display all icons in the notification area.



Click the icon brings up a menu of devices connected. Select the device used for the SOS backup.



If Windows is able to close all the files on the device you get a message indicating it is safe to disconnect the device. Otherwise you will get a message telling you it is not safe. Try after a little while until you get the message that it is safe.



Safe To Remove Hardware

The 'USB Mass Storage Device' device can now be safely removed from the computer.

7) **FINAL STEP**: Take your backup off premise or place in a fire retardant box. A backup is no good if it is lost, damaged, or ruined in a natural disaster.

Devices

Two excellent choices for backing up SOS data are a USB hard drive or a USB memory stick.

The USB memory stick used for backing up your SOS data go by various names: memory stick, thumb drive, flash drive, or jump drive. They are units about 2" long, 3/4" wide and 1/4" thick, i.e. smaller than a tube of lipstick. They come in various capacities, but today 4 GB is pretty standard. USB Memory sticks are inexpensive compared to USB hard drives. The pros using memory sticks include easier to store in a desk drawer, safe, and safety deposit box. One con using memory sticks is that they are easier to lose and are easier to be stolen.

USB hard drives are a good alternative. They are going to hold more information (running into terabytes). They do the same job as the memory sticks, but are more expensive.

Advice shared from Sue Cunningham: Do NOT trust your data to the brand IMATION for USB drives. Way too many SOS customers report failures.

CD drives are **NOT** recommended. They can easily scratch, their software can be quite temperamental, and they don't do well in using them much beyond one time only.

Cost-wise, USB memory sticks will be the most economical in the long run. This is what most of the stores running SOS use, so the instructions will accommodate accordingly.

How much space is needed on the backup device?

The amount of space is going to depend on how much information you have stored in the SOS data files. The files are compressed into a ZIP file. The size of this file also depends on the level of encryption and the type of information in the data files.

USB drives come in various capacities; most today start around 4 GB of data. It is recommended to have one USB drive this size or greater for each day of the week that you are open.

WITHOUT ANY DATA, a full backup of SOS (all programs, all reports, all data, etc.) occupies about 100 MB of space. You should always have at least one USB drive that contains a full backup of all SOS information - programs, reports, data, etc. That makes re-installation of SOS a snap if your computer suffers any hardware problems. You'll be up and running again in less than 10 minutes if you have to restore SOS or move SOS to a new computer.

Multiple Devices for offsite backups

Backups retain the data as long as the files are kept safe. If you use one device and it holds one backup and that backup or the device is somehow bad, you have no backup. For this reason, we recommend having numerous backup copies.

Minimally you should have three backup devices for rotation of backups, but the more you have including device marked “Monday”, “Tuesday”, “Wednesday”, etc., and another marked “weekly”, and another marked “monthly” that can be rotated in. An article from Wikipedia (http://en.wikipedia.org/wiki/Backup_rotation_scheme) explains different schemes and approaches.

Offsite options

Taking a backup offsite is very important. Minimally, a trusted employee (owner, board member, high-level manager, etc.) can take the backup device home with them each night. This way if the office has a fire, or severe weather harms the facility, or a break-in occurs, and the computer is destroyed or stolen, the data is safe elsewhere.

But taking it home means it is vulnerable to theft or the same severe weather event. And what happens if the trusted employee leaves the organization?

One basic way to protect the data is to place the external device into a safety deposit box at a local bank. The bank safety deposit boxes are secured and protect against basic weather events. It is not a perfect-perfect situation, but is definitely protects against 99% of the possibilities. It is important to consider however, the backups can only be retrieved during the hours the bank is open.

There are several services now marketing “cloud backups” where the files are stored on a remote computer. The files get copied to the remote computer using the Internet. This approach provides very secure backups. It removes the threat of localized weather events taking out the facility and the bank or home, and is normally retrievable anytime day or night. There are a number of things to consider when taking this approach.

1) Requires a fast broadband Internet connection
2) These types of services normally charge monthly or annual fees.
3) If the service decides to terminate your contract, or they go out of business, your historical backups could be lost.
4) Also, we recommend encrypting the backups in case the service provider is hacked and the hacker finds a way to get all the data.
5) Restoring the data is only as fast as the remote servers and your Internet connection.

We do not have any specific recommendations, but here is an interesting article covering numerous providers:

http://pcsupport.about.com/od/maintenance/tp/online_backup_services.htm

The ultimate offsite backup scheme is likely a combination of a safety deposit box and a “cloud backup”, but we recommend working with your local IT service provider to come up with the best scheme for your organization.

Full machine backup tools

While it is ultimately important to back up your SOS data, you also might want to take a broader approach to backups. You can backup or image entire computers to protect from a catastrophic drive failure. These backups are known as imaging because in the case of a complete disk drive failure you can get a new hard drive, and restore the entire image back to the disk and be back up and running quickly.

If you are taking this approach, we recommend you get advice from a local IT service provider. These folks can make professional recommendations to your particular situation and configuration. Choices and offerings in disaster recovery vary depending if you are running a server, number of workstations you have, etc. If you are looking for tools we can recommend a couple to consider:

StorageCraft's ShadowProtect: http://www.storagecraft.com/

Acronis' True Image: http://www.acronis.com

How to contact SOS support:

Email:	SOS@WhiteLightComputing.com
Phone:	307.745.4020 (Mon-Fri 10:00AM-6:00PM ET), emergency weekends
FAX:	307.745.8787
Web:	http://Antiques-SOS.com