BACKING UP OPEN AND LOCKED FILES

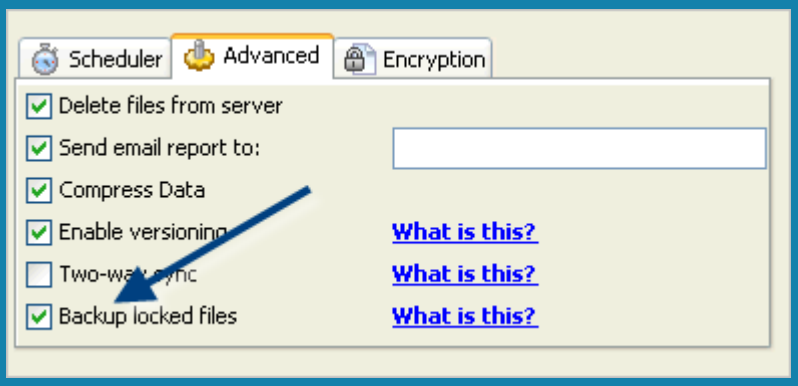
SchoolsVault has the ability to backup opened and locked files. This feature only applies when running on Microsoft Windows platform.

VOLUME SHADOW COPY (VSS)

Many applications running on Microsoft Windows OS can choose to lock their data files. This often create problems when other applications, such as SchoolsVault Client, want to read these files during a backup. Volume Shadow Copy (or VSS), is a technology included in Microsoft Windows that allows the OS to take manual or automatic backup copies (aka, snapshots of data) even if the file is locked, on a specific volume at a specific point in time over regular intervals.

ENABLING VSS IN SCHOOLSVAULT

VSS is automatically enabled in SchoolsVault when you check the box for **Backup Locked Files**. See the image below.



PREREQUISITES FOR USING VSS

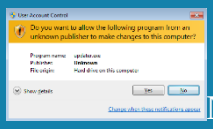
The following prerequisites must be met before using this feature:

Operating System

You must be using SchoolsVault Client on Windows XP, 2003, Vista, Windows 7, 2008, or Windows 8. VSS is not available on Windows 2000.

User Privileges

Using VSS on Windows is considered a privileged task available to users belonging to the **Administrator** group. Therefore, ensure that you are using a User account with enough privileges.


No additional steps are required if SchoolsVault Client is running on Windows XP or Windows 2003.

Extra steps are required, however, if you are running SchoolsVault Client on Windows 7, Vista, 2008, or Windows 8. These steps satisfy the restrictions imposed by UAC., which limits software to run under standard privileges until an administrator authorizes an elevation.

Backup jobs are typically run in the background without any human interaction and therefore, it is not practical for someone to click **Yes** to the UAC prompt displayed by the OS.

You have one of two options when dealing with UAC:

1. Disable UAC. Click here for more information.

OR

2. Run the backup task as **NT AUTHORITY\SYSTEM**, instead of the regular User. If a backup task is run using **NT AUTHORITY\SYSTEM**, UAC will not prompt the User for additional privileges.

Required Services

VSS requires the following services to be running on Windows:

- COM+ System Application
- Distributed Transaction Coordinator

SchoolsVault Client will attempt to start these services if they are not running, provided the User ID has enough privileges.

OS Architecture

You cannot use the 32-bit version of SchoolsVault Client if you are running on a 64-bit version of the OS. You must download the 64-bit version of SchoolsVault Client in order to use VSS. VSS does not work with Windows WOW (Windows on Windows).

USING TWO-WAY SYNC WITH VSS

VSS creates a read-only copy of the locked files. Therefore, SchoolsVault won't be able to fetch a newer copy from the Server if the file on the Client is locked. In such cases, you will see an error in the log file, and SchoolsVault will skip the file.

DISADVANTAGE OF USING VSS

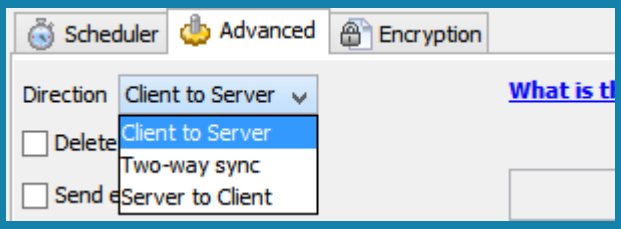
The amount of time it takes for a backup to complete increases significantly when you use VSS. This speed difference is more prominent if you have large files. This is because SchoolsVault needs to calculate the MD5 signature of every file during a backup. To speed up the matching process, these signatures are cached for files larger than 10 MB. This cache is not used when using VSS, which can significantly slow down the matching process.

Therefore, we recommend you use this feature only if you are sure you have open and locked files. Moreover, consider creating separate profiles for files that are locked, and for files that may be opened but not locked.

BACKUP DIRECTION

By default, files are copied from the machine where SchoolsVault Client runs to your SchoolsVault Server. However, SchoolsVault also allows you to copy files in both directions.

You can select how files are copied by using the **Direction** option in SchoolsVault Client.



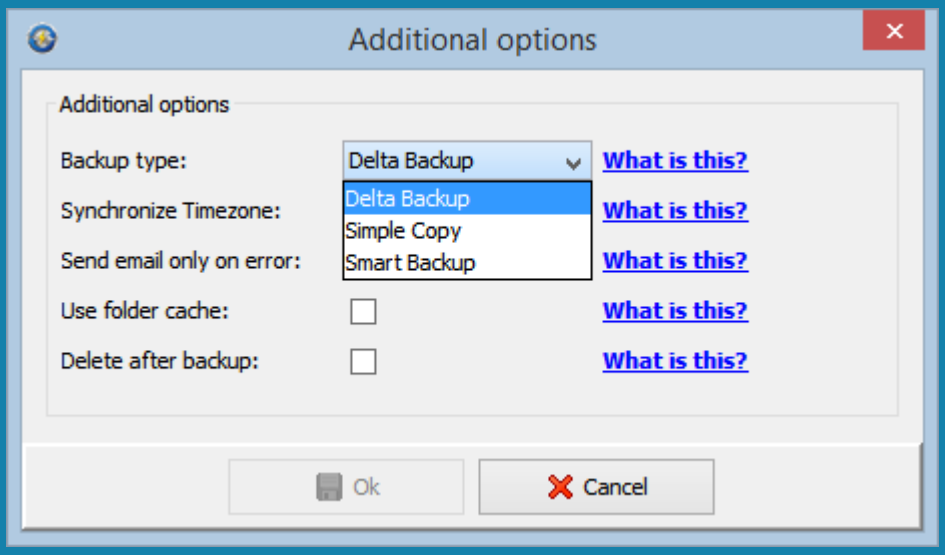
The following table describes what each option means:

Direction	Description
Client to Server	This is the default behavior. When a backup is run, newer files on the Client machine are backed up to the Server machine. No files are copied from the Server to the Client. If **Delete Files** is checked, files deleted on the Client will be deleted from the Server as well, unless Delete Retention has a value greater than 0.
Two-Way Sync	Newer files are copied in both directions - meaning if a new version of a file exists on the Server, it will get copied (or restored) to the Client. Similarly, a new file on the Client will get copied (backed up) to the Server. The Delete Retention option has no affect when Two-Way Sync is enabled. This option is NOT available in the Personal edition of SchoolsVault.
Server to Client	Files on the Server are copied to the Client if they are different. This is similar to running a restore operation, but with one difference: If **Delete Files** is checked, local files on the Client will be deleted if they do not exist on the Server.

This option is NOT available in the Personal edition of SchoolsVault.

BACKUP TYPES

Different backup types provide finer control over how files are copied to the destination Server. This is specified by selecting one of three values for Backup Types.



The following table describes what each type means:

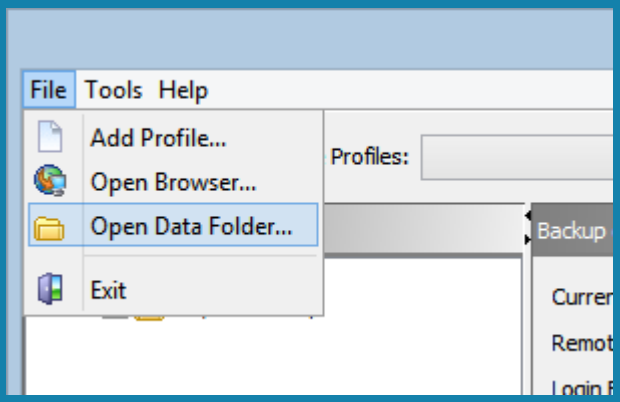
Backup Type	Description
Delta Backup	This is the default backup type, and it uses the rsync algorithm to determine the differences between files, then sends non-matching blocks over the network.
Simple Copy	Using this option disables rsync and will force the Client to send the entire file, skipping the block matching process. You should only use this option if both SchoolsVault Client and Server are on a very fast network, such as the same machine or LAN.
Smart Backup	In this case SchoolsVault will switch between Delta Backup and Simple Copy, depending upon the file size and network. For example, if you have a 1 GB file on the Server, and the file size on the Client is 10 MB, it would be much quicker to transfer the entire 10 MB across the wire rather than matching blocks on a 1 GB file. **IMPORTANT:** Smart Backup is switched to Delta Backup if: • Backup Direction is set to either **Two-Way Sync**, or **Server-To-Client** • Versioning is enabled.

DATA FOLDER FOR SCHOOLSVAULT CLIENT

The Data folder in SchoolsVault is a special folder where information about every Profile is stored. In addition to Profiles, it also stores:

- **Log files** - these are stored in a sub-folder called logs
- **MD5 signatures** - these are stored in sigCache folder
- **Lock files** - these are temporary files that prevent a single profile from running simultaneously

The easiest way to get to the Data Folder is to click **Open Data Folder** item under the **File** menu in SchoolsVault Client.



ABSOLUTE PATH FOR DATA FOLDER

On Windows XP, 2003:

```
c:\Documents And Settings\YourUserName\.syncrify\
```

On Windows Vista, 7 & 2008

```
c:\Users\YourUserName\.syncrify\
```

On Linux, UNIX & Mac OS X

```
~/.syncrify
```

PREFERRED PATH

The preferred path on Windows platform is the **All Users** folder, instead of the individual user. The exact path is:

On Windows XP, 2003:

```
C:\Documents and Settings\All Users\SyncrifyData\
```

On Windows Vista, 7, 2008 & 8

```
C:\ProgramData\SyncrifyData\
```

Location of the Data Folder remains to be the on User's home directory for Linux, UNIX and Mac OS X.

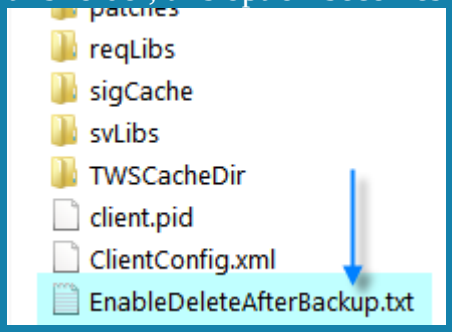
DELETING FILES AFTER BACKUP

When this option is enabled, SchoolsVault will delete files on the Client after they have been successfully backed up. This option is only valid when the Backup Direction is Client-to-Server. It has no effect when the backup direction is either Server-to-Client or Two-Way Sync.

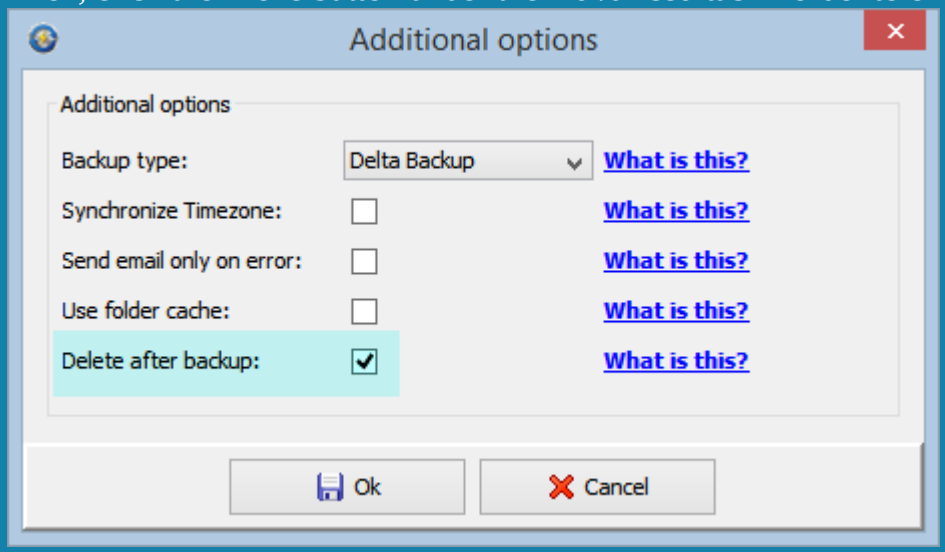
DANGERS IN ENABLING THIS FEATURE

Enabling this option can be very dangerous since it has the potential to delete important files from the machine. As an added precaution, this feature is disabled by default.
In order to enabled it, you must do the following:

- Start SchoolsVault Client
- Click **Open Data Folder** under the **File** menu
- Create a new Text file called **EnableDeleteAfterBackup.txt** in this folder. The contents of this text file does not matter, you can leave it empty. As long as SchoolsVault sees this file in this folder, this option becomes accessible.



- Then, click the **More** button under the **Advanced** tab in order to enable this feature.



IMPORTANT

Files on the Client are only deleted if they have been successfully transferred to the Server. Additionally, if the **Delete Files** option is checked, this feature will be disabled.

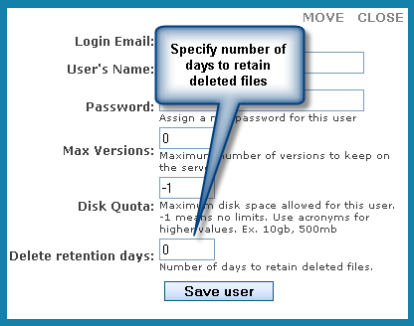
DELETE RETENTION PERIOD

SchoolsVault Client has the option of deleting files from the Server if the corresponding file is deleted from the Client. If a user deletes a file by mistake on the Client and runs a backup, SchoolsVault Server will remove that file from its repository, and the file can never be recovered.

A parameter called **deleteRetentionPeriod** allows SchoolsVault Server to retain deleted files for a certain number of days. The default value for this parameter is 0, which means that files will be deleted from the Server when a backup is run. A value greater than 0 indicates the number of days you want to retain a deleted file. For example, if you specify 10 for this value, every file that is deleted on the Client is held by the Server for the next 10 days, allowing the User to restore it if needed. It will be deleted from the Server after 10 days.

STEPS TO ENABLE THIS FEATURE

- Log in to SchoolsVault's Web Interface as **admin**
- Click on **Manage Users**
- Click on the **Modify** link for the desired user. This will open the following pop-up window:



- Specify a positive number for **Delete Retention Days**

HOW IT WORKS

When the value for **deleteRetentionPeriod** is specified to be greater than 0, the following occurs:

- Files that are deleted from the Client machine get marked for deletion. They won't be deleted right away.
- An email report is sent to the User, which indicates that the file has been deleted. This email allows the User to restore the file if it was deleted by mistake on the Client machine.
- The file can be restored until the Retention Period days has expired.

DISASTER RECOVERY / RESTORING A PROFILE

The following steps demonstrate how to restore files from SchoolsVault Server to a Client machine that has been recently rebuilt from a crash.

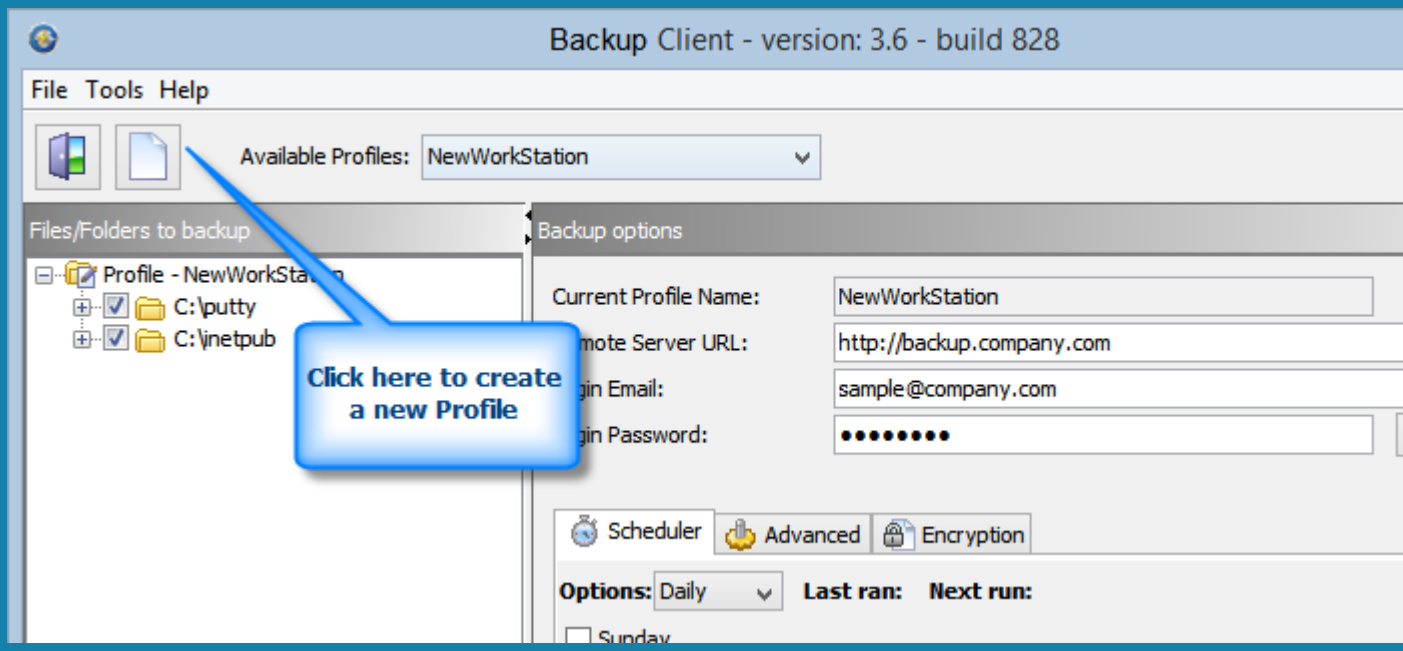
ASSUMPTIONS

- The host name of SchoolsVault Server is **backup.company.com** and is listening on port 80
- The original Profile Name is **WorkStation001**
- The host name of the newly-built machine is **NewWorkStation**

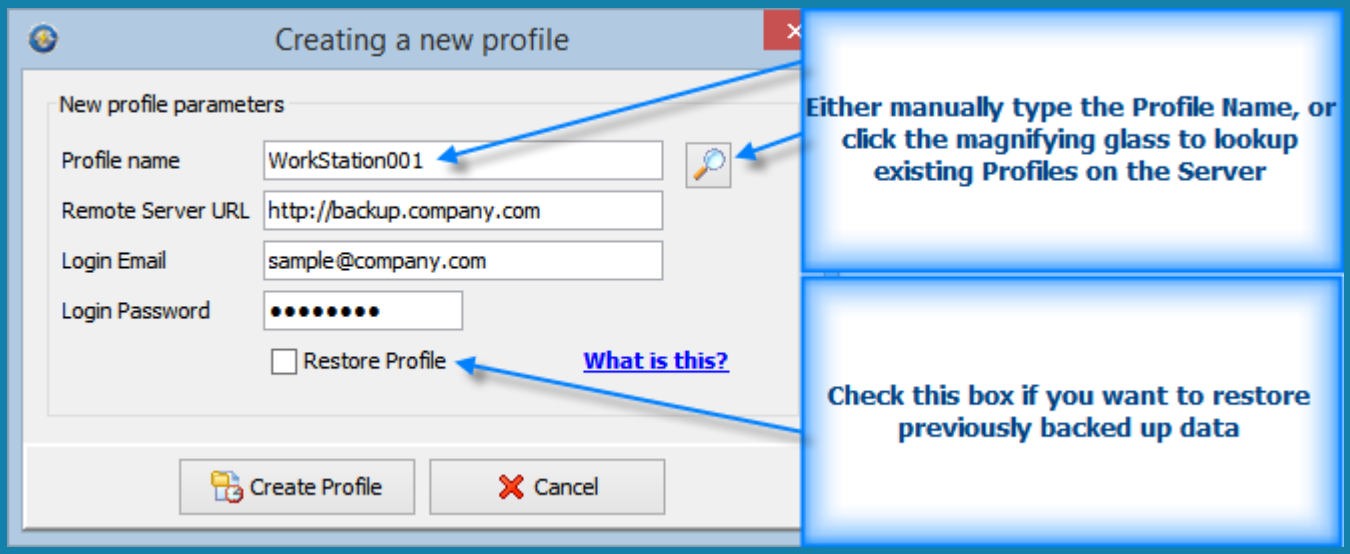
STEPS

1. Specify http://backup.company.com for Remote Server URL, as well as your login email and password.

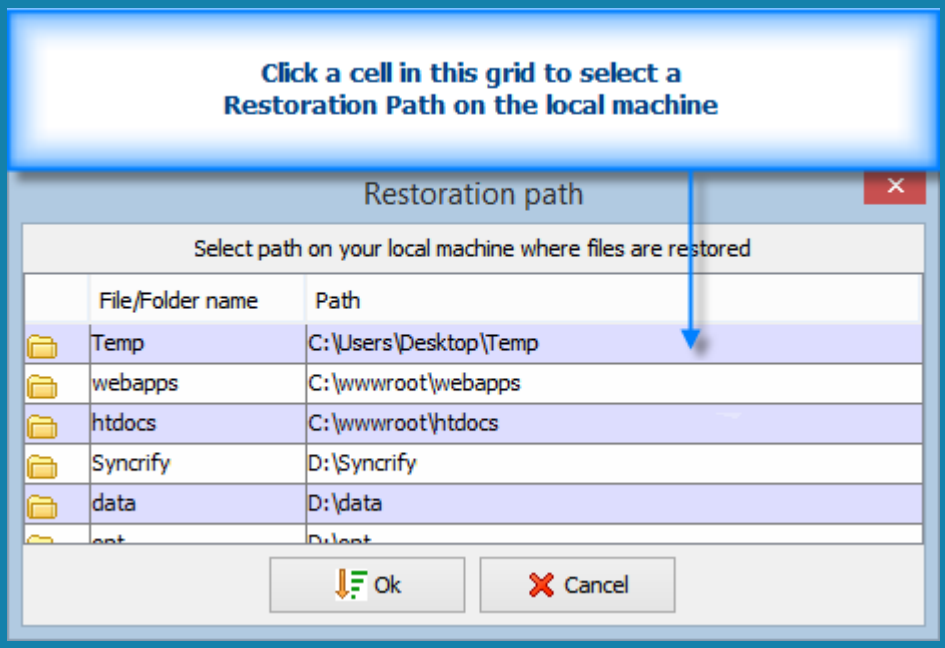
2. When you first start SchoolsVault Client on this new machine, it will automatically create a default profile called **NewWorkStation**. This is because the Client creates a Profile based on the machine's host name. Since you are restoring data, create a New Profile called **WorkStation001**



3. The following screen displays how to create a New Profile. You can either type **WorkStation001** manually, or click the search button to display a list of existing Profiles associated with your User ID on the Server.



4. When **Restore Profile** is checked, you will see the following screen.



This screen allows you to specify a different location for folders in the Profile. Consider the scenario when you were using Windows XP in the past and are now moving to Windows 8. Several folders on Windows 8 have a different name. For example:

- **C:\Documents and Settings\John\My Documents** - Windows XP
- **C:\Users\John\Documents** - Windows 8

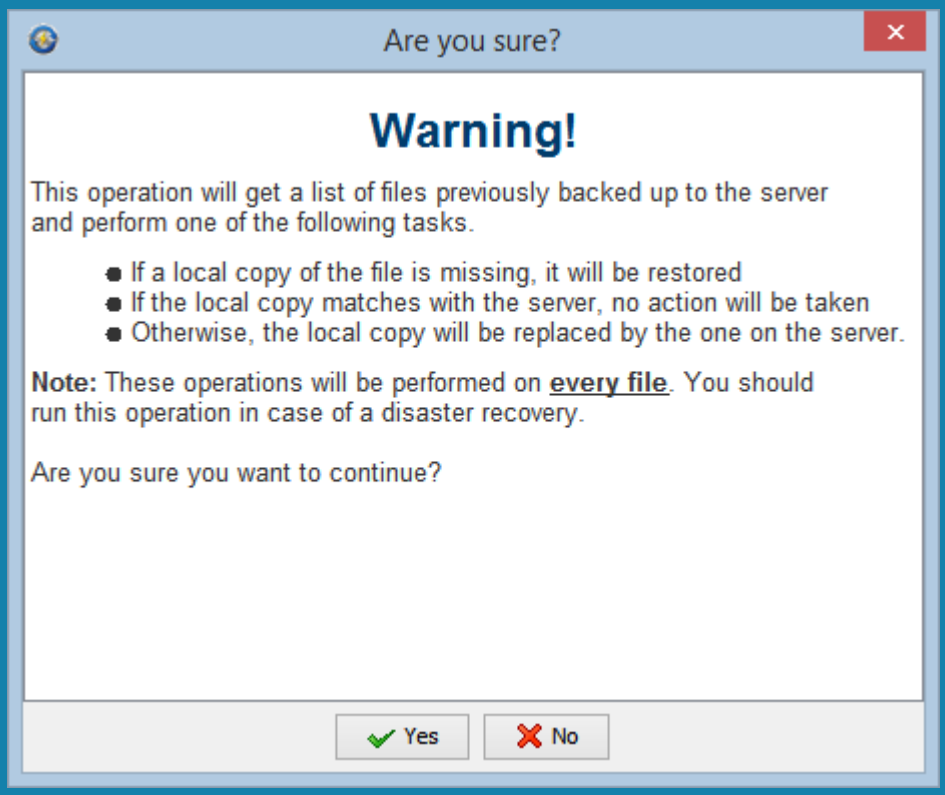
Using this screen you can specify a different location for such folders.

VERY IMPORTANT

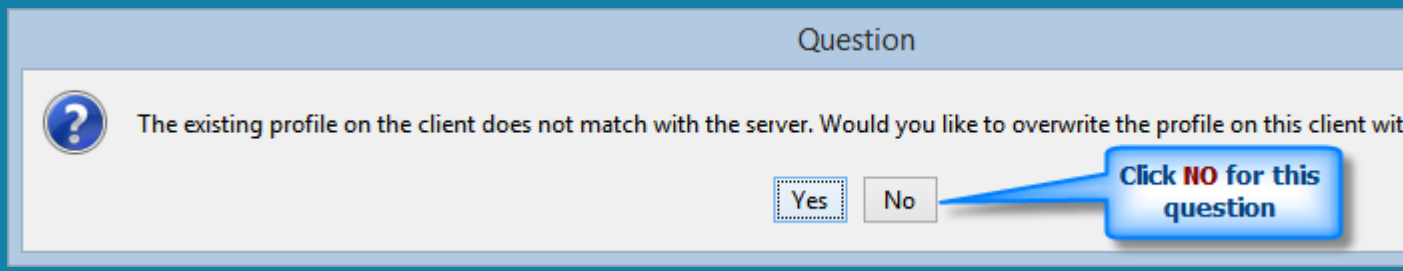
Ensure the last folder name in the new path matches with the value in the first column. For example, if the first column says **webapps**, the absolute path in the second column should be C:\wwwroot**webapps**, not C:\wwwroot. This ensures files are copied to the correct folder.

5. Once a Profile is created, either click the Restore button or right-click on the left hand side of the GUI to bring up the pop-up menu, then select Restore ALL files

6. You will get a warning message saying local files will be replaced by the version that exists on the Server. Click **Yes** to this question as well.



7. If you specified a different location for the target files in Step 4, you will be prompted with the following question:

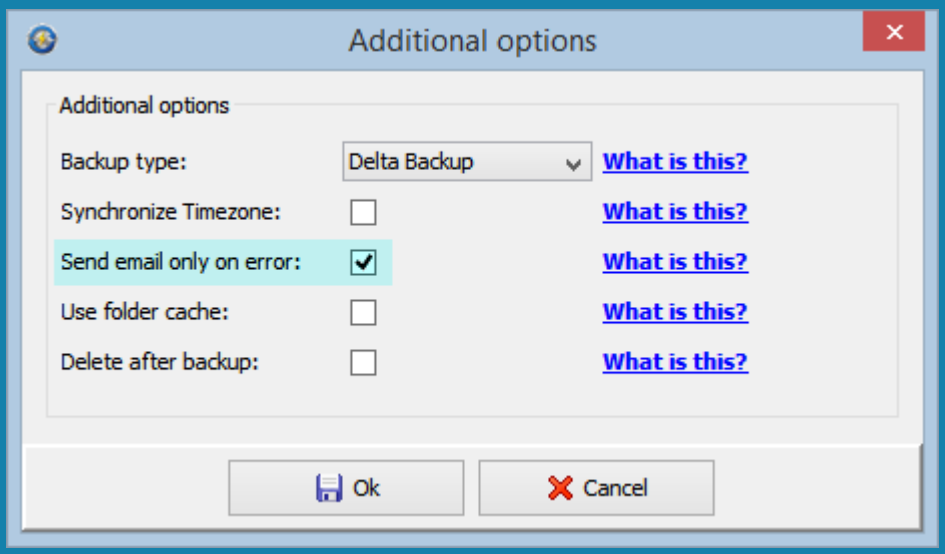


8. That should be it. SchoolsVault Client will first download the Profile information from the Server and will then download files.

EMAIL OPTIONS IN SCHOOLSVAULT

Once a backup job is complete, SchoolsVault Client can send an email to the User, which contains a list of files that were modified. This email is sent only when you run a backup from the console or via the scheduler. An email is **not** sent when running backups manually.

By default, emails are generated regardless of the results - even if there are no errors. Although many Users may like getting emails regardless of the status of the backup, some may prefer getting it **only** if an error occurs.



Enabling the check box (as shown in the image above) does exactly that. SchoolsVault will only generate an email if one or more errors occur during the backup.

IMPORTANT

SchoolsVault Client never sends an email to your SMTP Server. Instead, it prepares the email body, then sends it to SchoolsVault Server, which then contacts the configured SMTP Server. Therefore, it is important for the Administrator to correctly configure the SMTP settings on SchoolsVault Server.

USING ENCRYPTION WHILE BACKING UP FILES

Users can backup an encrypted version of the files to the server. When files are encrypted they cannot be seen/opened by anyone unless they know the password that was used to encrypt it.

IMPORTANT

- Ensure that you have read this article in its **entirety** before using this feature.
- This tool does not change the file name when it is either encrypted or decrypted.

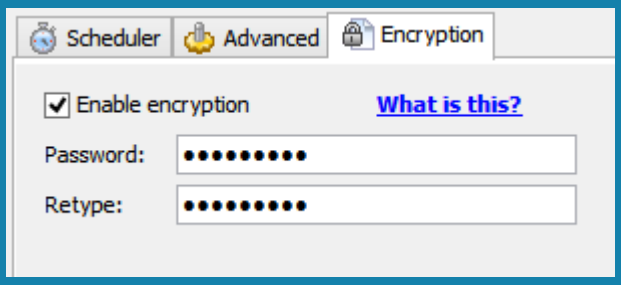
PROS AND CONS OF USING ENCRYPTION

The **benefit is obvious: the only reason you would want to encrypt any file is to prevent non-authorized users from accessing it**. Below are some disadvantages of using this features.

- **Speed** - When you encrypt files, backups will run slower. Every file that needs to be backed up will be encrypted on the client's end and then will be sent to the server. This time delay is particularly noticeable for large files. For example, encrypting a 1GB file can take approximately 3 minutes.
- **Lost password** - You will NOT be able to recover your file from backup if you forget the password. Syncrify uses 128 bit strong AES encryption to encrypt files. This type of encryption can take years even for a computer to guess a password.
- **Entire backup** - Every file from your local machine gets copied again if you
    - change your password
    - switch from encrypted to unencrypted mode or
    - unencrypted to encrypted mode.
- **Restore** - Syncrify client will be able to restore files without any extra steps. However, if you use the browser to download a file from the server, you will have to manually decrypt it using Syncrify client.

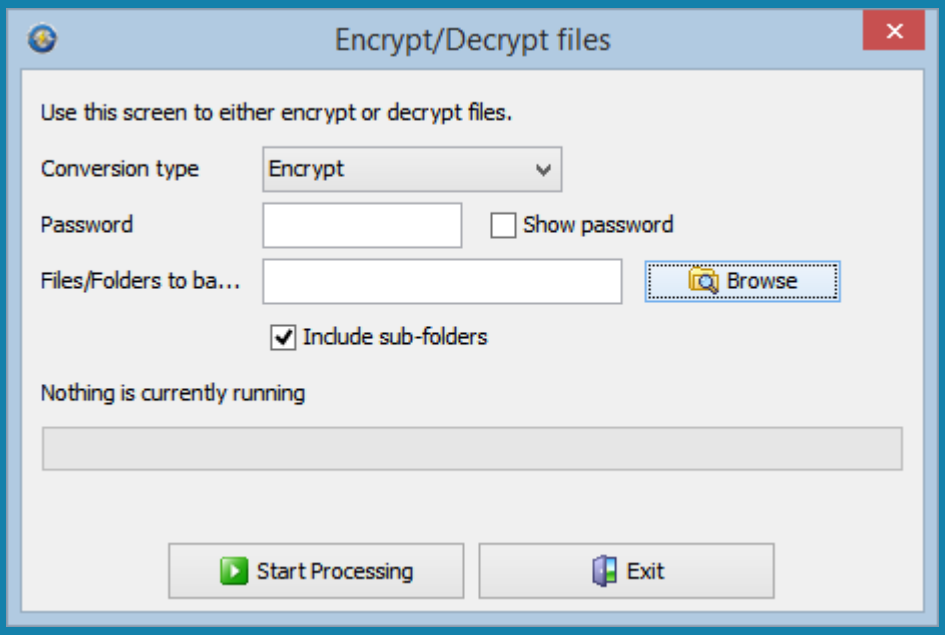
HOW TO USE ENCRYPTION

To use encryption simply click on the encryption tab, select the option for encryption and specify a password. The password cannot be more than 16 characters long. Refer to the image below.



ENCRYPTION TOOL IN SYNCRIFY CLIENT

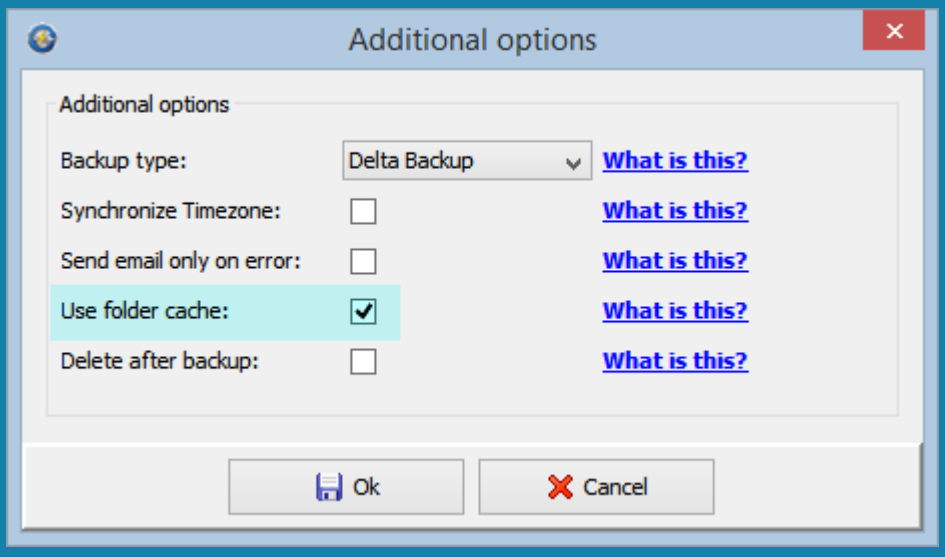
For your convenience, Syncrify client includes a tool that can be used to encrypt/decrypt files on demand. Click **Encrypt/Decrypt files** from the Tools menu. This opens the following screen.



This screen is used to either encrypt/decrypt a single file or every file in a folder. When Include sub-folders is checked, files will be included recursively.

LOCAL CACHE ON THE CLIENT

SchoolsVault Client compares folders on the local machine with the corresponding folders on the Server in order to determine whether or not it contain files that require a backup. This is the default behavior, and it is done for every folder on the Client machine.



When the Folder Cache option is enabled, SchoolsVault creates a local cache file on the machine. This cached data is stored in a sub-folder called **FolderCache** off of the Data Folder.

BENEFITS

- **Speed** - Using the local folder cache reduces the total amount of time spent for backup. The amount of time reduced is directly proportional to the number of folders on the client machine - therefore you will see a significant time reduction for jobs containing thousands of folders. If the client does not have many folders, the speed reduction is not significant. During a test conducted in our labs, with a backup containing about 35,000 folders, we found the time reduced from 45 minutes to 6 minutes when local cache was used.
- **Scalability** - Increases Server scalability as less requests are sent from the Client to the Server. Due to this reason, it is a good idea to turn this option on if you are an ISP.

COSTS

If files are modified on the Server using any other channel, the Client will not know about them and therefore, a backup won't occur. For example, the last modified date of a file on a Client machine is January 01, 2010. If the same file on the Server is somehow modified on January 15, 2010, the client won't know about this change.

FORCING CLIENTS TO USE CACHE

Although every Client can determine if they want to use the local cache, the Server Administrator has the ability to force Clients to use it even if the Client decides not to. This is particularly useful if you are an ISP, and you want to make the Server more scalable.

IMPORTANT

Local Cache is not used when:

- Encryption is used
- Direction is either **Two-Way Sync** or **Server-To-Client**

REMOTELY CONTROLLING SCHOOLSVAULT CLIENT

REMOTE CONTROL ALLOWS ADMINISTRATORS TO:

- Manually trigger a backup on a Client machine from SchoolsVault Server's web interface
- Fetch log and configuration files from the Client machine allowing Administrators to troubleshoot problems.

PREREQUISITES OF USING REMOTE CONTROL

- Windows Service Client is installed. At this time, this feature is only available on Clients running on MS Windows. Mac OS X and Linux Clients do not have this feature.
- Ensure Remote Control is enabled. Click **Options** under the **Tools** menu in SchoolsVault Client, then check the box for **Remote Control**

USING REMOTE CONTROL FROM THE SERVER

- Login as **admin** to SchoolsVault Server's web interface
- Click **Remote Clients** under **Quick Links**
- Click **View Details** next to the desired Client
- The next page displays Profiles that are configured for this Client
- Click **Run Now** to trigger a backup.

IMPORTANT

- A manual backup can take up to a minute to actually start when triggered from the Server's web interface.
- SchoolsVault Client can connect to more than one Server to run backups. However, Remote Controlling can be done through one Server only. Consider an example where SchoolsVault Client runs **profileA** to **serverA**, **profileB** to **serverB** and **profileC** to **serverA**.

  In this example, only serverA will be able to remote control the Client. SchoolsVault Client picks serverA for Remote Control because it appears in two profiles, whereas serverB is used in one.

DISASTER RECOVERY / RESTORING A PROFILE

The following steps demonstrate how to restore files from SchoolsVault Server to a Client machine that has been recently rebuilt from a crash.

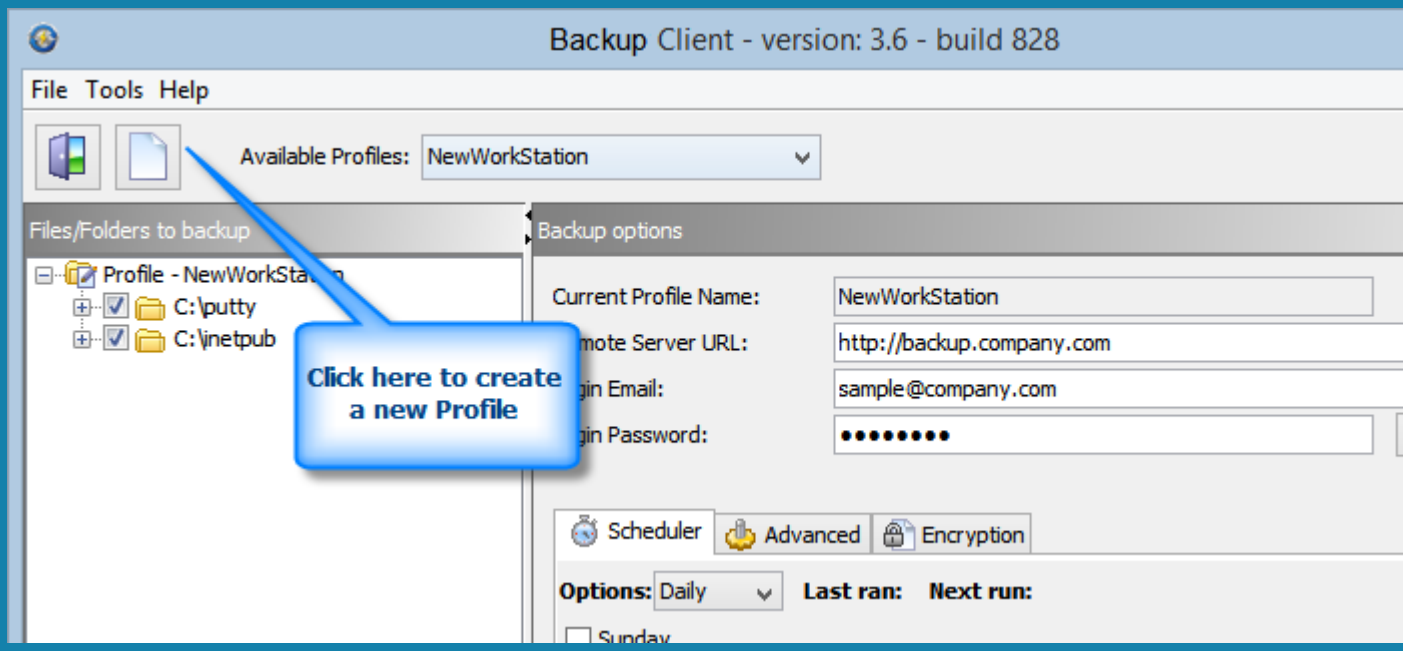
ASSUMPTIONS

- The host name of SchoolsVault Server is **backup.company.com** and is listening on port 80
- The original Profile Name is **WorkStation001**
- The host name of the newly-built machine is **NewWorkStation**

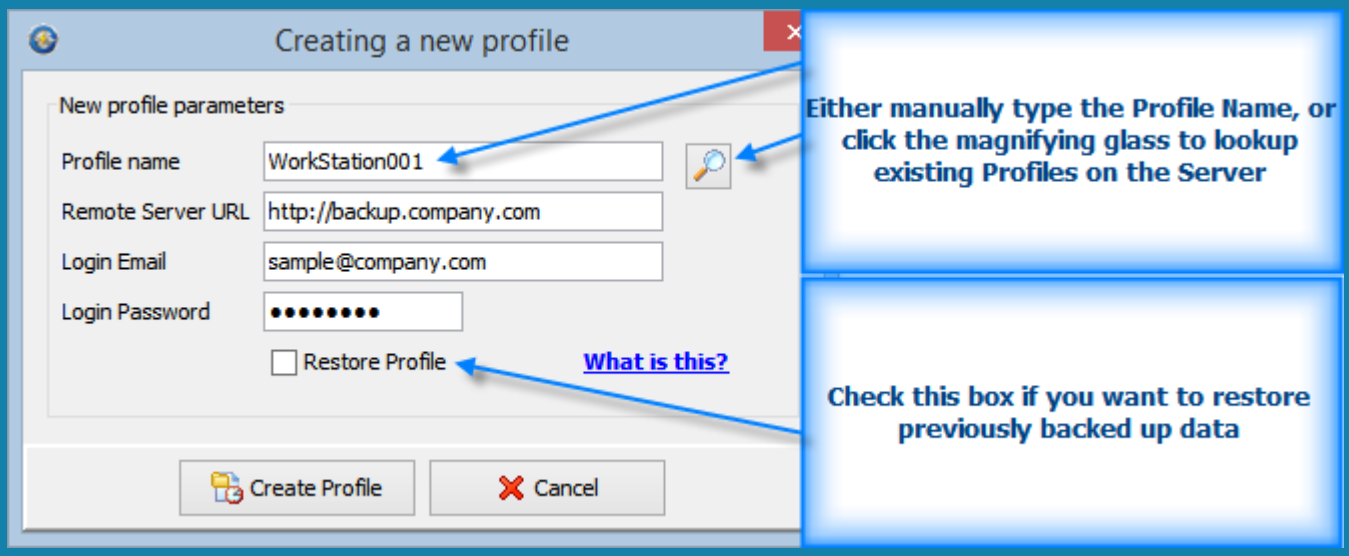
STEPS

1. Specify http://backup.company.com for Remote Server URL, as well as your login email and password.

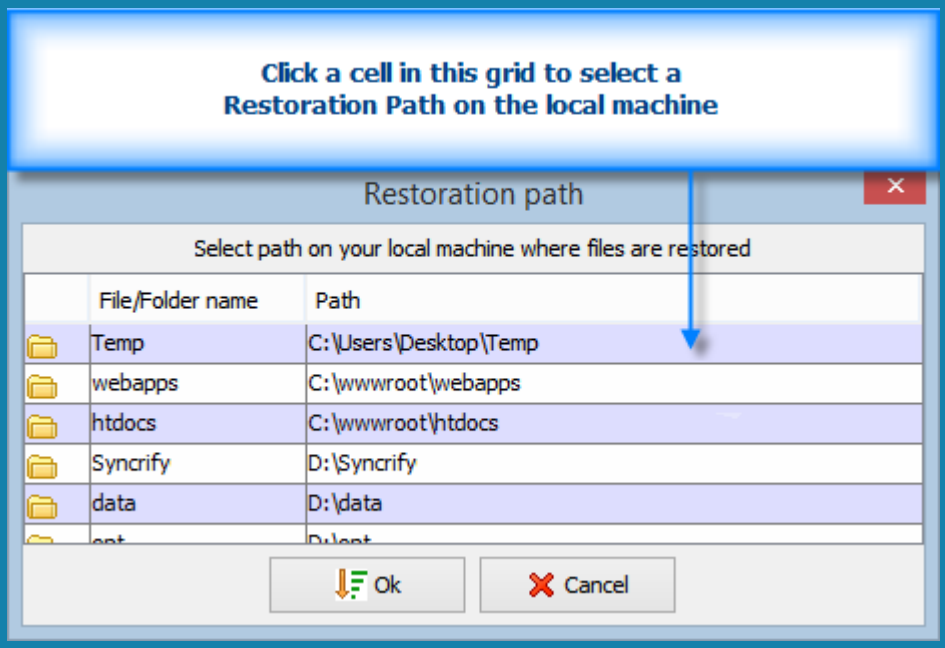
2. When you first start SchoolsVault Client on this new machine, it will automatically create a default profile called **NewWorkStation**. This is because the Client creates a Profile based on the machine's host name. Since you are restoring data, create a New Profile called **WorkStation001**



3. The following screen displays how to create a New Profile. You can either type **WorkStation001** manually, or click the search button to display a list of existing Profiles associated with your User ID on the Server.



4. When **Restore Profile** is checked, you will see the following screen.



This screen allows you to specify a different location for folders in the Profile. Consider the scenario when you were using Windows XP in the past and are now moving to Windows 8. Several folders on Windows 8 have a different name. For example:

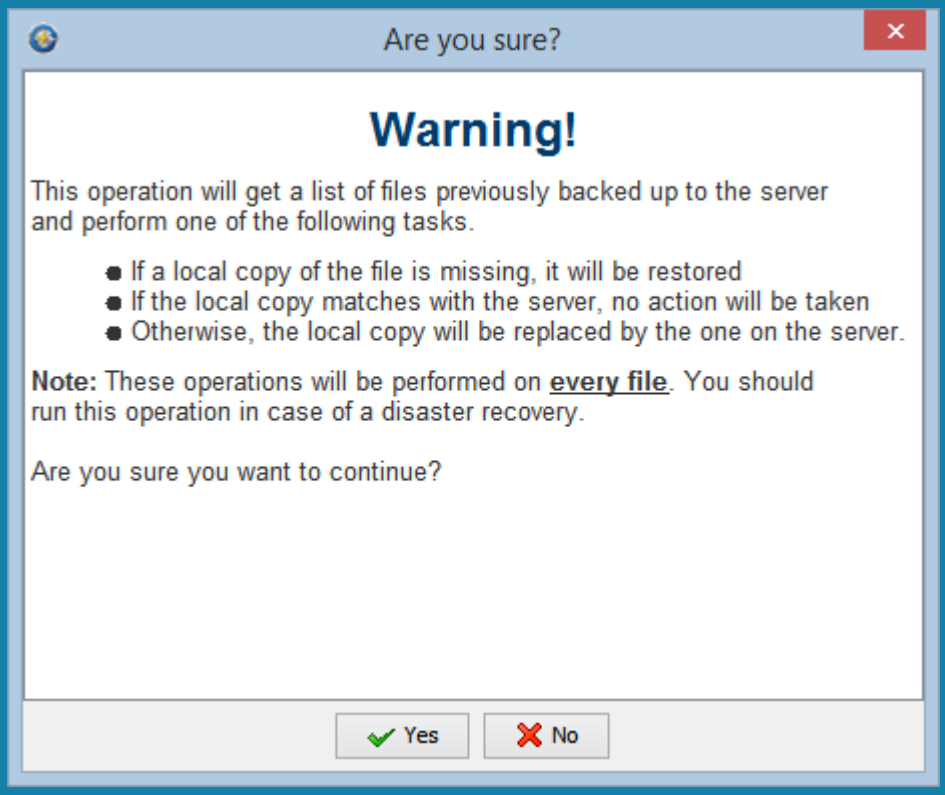
- **C:\Documents and Settings\John\My Documents** - Windows XP
- **C:\Users\John\Documents** - Windows 8

Using this screen you can specify a different location for such folders.

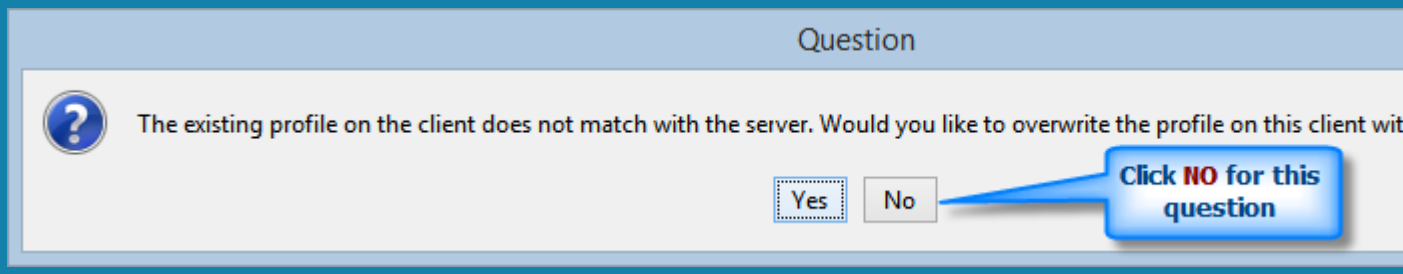
VERY IMPORTANT

Ensure the last folder name in the new path matches with the value in the first column. For example, if the first column says **webapps**, the absolute path in the second column should be C:\wwwroot**webapps**, not C:\wwwroot. This ensures files are copied to the correct folder.

5. Once a Profile is created, either click the Restore button or right-click on the left hand side of the GUI to bring up the pop-up menu, then select Restore ALL files
6. You will get a warning message saying local files will be replaced by the version that exists on the Server. Click **Yes** to this question as well.



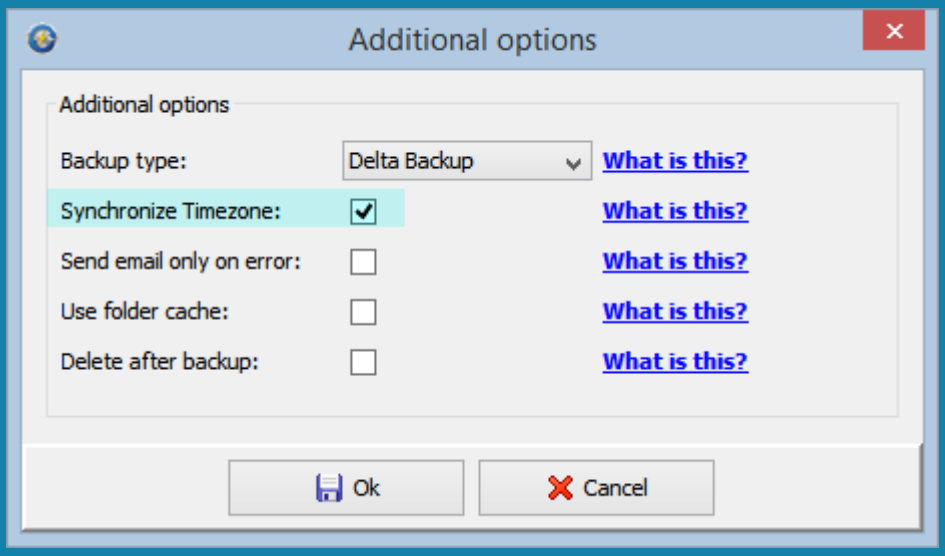
7. If you specified a different location for the target files in Step 4, you will be prompted with the following question:



8. That should be it. SchoolsVault Client will first download the Profile information from the Server and will then download files.

SYNCHRONIZE TIMEZONES

SchoolsVault is designed to work across different timezones. When this options is checked, files on the Server will use the same timezone that is being used on the Client. When this option is NOT checked, files on the Server are stored using GMT timezone.



CONSIDER THIS SCENARIO

- You are using SchoolsVault to synchronize folders on machines around the world.
- The Two-Way Sync feature is enabled, which means newer files will prevail
- Machine A is in New York
- Machine B is in California
- What happens at run-time? Refer to the following table:

Event	Option is checked	Option is not checked
A user in New York modifies a file at 3:00 PM EST.	The last modified date (LMD) for this file on the server will be 3:00 PM	The last modified date (LMD) for this file on the server will be 8:00 PM, since New York is on EST (-5 GMT)
A different user modifies the same file in California at 1:00 PM PST, which is 4:00 PM EST	LMD on the server will be 1:00 PM	LMD on the server will be 9:00 PM, since PST is -8 GMT
A backup is run with Two-Way Sync enabled	File is copied from the Server to the Client, and the changes made by the User in California are lost.	File is copied from the Client to the Server.

SUMMARY

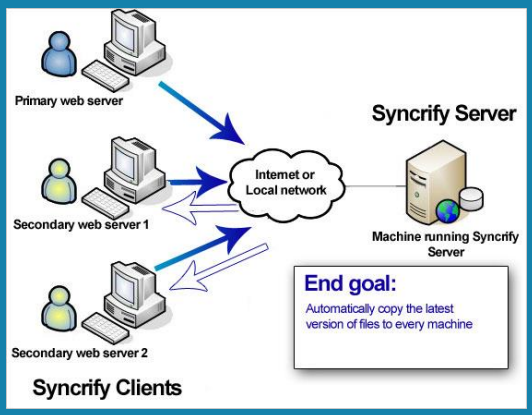
- Do NOT check this option if:
  - You have Clients in different timezones AND
  - They use Two-Way Sync to synchronize files.

IMPORTANT

Consider **Initialize Seeding** if you change this option, which will ensure that the LMD on the Server is correctly specified. Click **Initialize Seeding** under the **Tools** menu to start this process in SchoolsVault Client.

TWO-WAY FILE SYNCHRONIZATION

Often users have to synchronize contents of two folders on two different machines. Two-Way Synchronization helps you to achieve this goal.



Consider a scenario where you have multiple web servers. You have one primary server and two other secondary servers. If a file changes on the primary server, you want that file to propagate to the secondary servers. This way, in an event of a failure, you can redirect users to one of the secondary servers.

SOLUTION

You can enable the Two-Way Synchronization option, which allows SchoolsVault to not only backup files from Client to Server, but it can also automatically update older files on the Client with a newer version on the Server (if it is available).

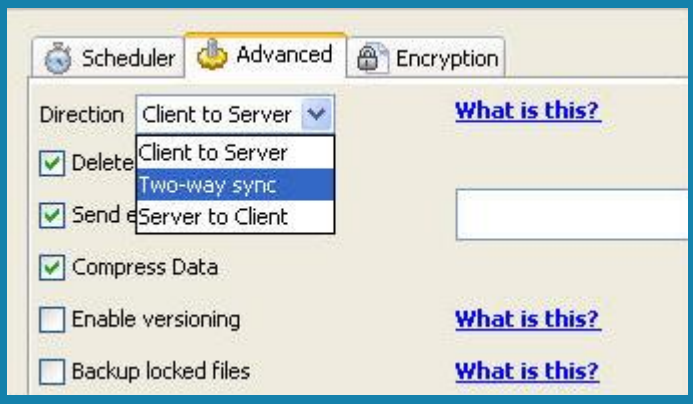
LET'S ASSUME THE FOLLOWING:

- You created a new file on the primary web server.
- When a backup is run on the primary web server, this file will get copied to SchoolsVault Server, which is used to hold your backup data.
- When a backup is run on the secondary web servers, this file gets downloaded to the Client machine since it does not exist.
- If you change the contents of this new file on any machine, the newer version will get copied to every other machine

STEPS TO USE THIS FEATURE

The following steps assume you want to synchronize the contents of the **C:\wwwroot** folder between all 3 machines.

- Create a new Profile on your primary web server. Let's call this Profile **WebProfile**.
- Add **C:\wwwroot** to this Profile
- Select Two-Way Sync for the direction field.



- Save the Profile
- Create the same Profile on the other two secondary servers.

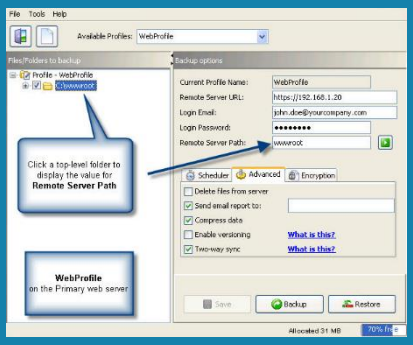
IMPORTANT

Make sure to use the same name for the Profile on all three web servers.

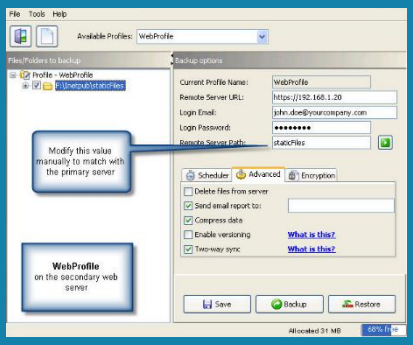
ADVANCED SCENARIO

Often you want to synchronize folders with different paths. For example, the absolute path on your primary web server is **C:\wwwroot**, but you want to use the **F:\Inetpub\staticfiles** folder on the secondary server. The following images display a screen shot of SchoolsVault Client on both machines.

Primary web server



Secondary web server



When you add folders to a Profile, SchoolsVault Client automatically assigns a value for **Remote Server Path**, which is typically based on the leaf folder name. If the absolute paths are different between primary and secondary web servers, you will have to manually change this value to match with the primary machine.

SUMMARY

The following must match on every machine where you want to use the Two-Way Sync feature.

- You must use the same user to run the backups
- Profile names must match. (Profile names are case-sensitive)
- Value for **Remote Server Path** must be same between every Client machine
- Check box for **Two-Way Sync** must be checked
- Values for **Compression** and **Versioning** must be same across every Client.

CAVEATS

Delete retention option is disabled when using Two-Way Sync. Additionally, following statements are true:

- You have 3 Client machines that backup a Profile using Two-Way Sync. SchoolsVault will ensure that files on these 3 machines stay synchronized
- Besides these Client machines, a copy will also be stored on SchoolsVault Server.
- If one of the Clients deletes a file, then that file will be deleted from the other 2 Clients as well as on the Server.
- Files should never be deleted directly from the Server's repository. If a file is deleted on the Server, it will simply reappear on the Server. If you want to delete a file, you should always delete it from the Client's end.

CREATING FILE VERSIONS

Multiple versions of a file can be created on the Server. Consider the following scenario:

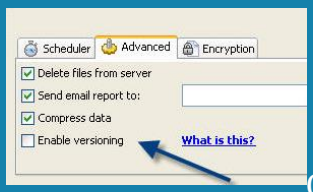
- A user creates a new document and backs it up to SchoolsVault Server
- Later on he/she makes changes to this document and backs up the modified version of the same file
- SchoolsVault Server will keep both versions of the file. The latest version is stored as-is on the Server, but older versions only contain the difference in the file. If a user decides to restore an older version, SchoolsVault Server will rebuild the file on-demand.

BENEFITS OF USING VERSIONING

- Users can restore a previous version of a file.
- Previous versions of a file are stored in a special format containing enough information to rebuild the file on demand, which reduces the amount of used disk space on the Server tremendously.

STEPS TO USE VERSIONING

Versioning can be enabled or disabled on a per-user basis. When creating a new user, the administrator must decide the number of versions to maintain for every file. Specify a number greater than 0 to enable Versioning. Assume a backup is run every night. Specifying a value 7 for this field will create up to 7 versions of a file, each representing one day of data.



On the Client's end, Versioning can be further narrowed down to a Profile level - meaning you can select the Profiles for which Versioning is enabled. This allows Users to create versions of files/folders that require it, while those that don't require versions can be backed up in a different Profile.

Follow the steps below to enable Versioning on the Client's end:

- Start SchoolsVault Client
- Select a desired Profile
- Click on the advanced tab
- Check Enable Versioning
- Save the Profile

CAVEATS

It is important to note that previous file versions are automatically deleted when:

- File Encryption is enabled or disabled
- Encryption password is modified
- Versioning is enabled on the Server, but the Client runs a backup job with this option disabled. In this case, the previous versions will be removed and new versions will be created when it is enabled again.
- The option "**Delete files from Server**" is checked, and the User deletes a file from the Client machine.

RESTORING PREVIOUS VERSIONS

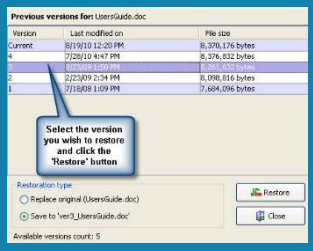
Previous versions of a file can only be restored using SchoolsVault Client. You **cannot** use a web browser to restore an older version of a file

Following steps demonstrate how to restore a previous version

- Start SchoolsVault Client
- Navigate to the file that you would like to restore. If the desired file does not exist on the Client, create a dummy file with the same name
- Highlight the desired file, click the right mouse button, then select **Restore Previous Versions** from the pop-up menu.

- This will invoke a screen that displays all previously backed up versions, and it allows Users to restore the desired file.

This screen displays all previous versions of the selected file in a grid, which contains the following information:



- **Version** - Version number of the file. Version numbers are incremented whenever a new version is backed up. Assume you decide to store 10 versions for every file. In this case there will be a maximum of 11 files on the server - 10 files containing deltas (differences) for the older versions, and one file representing the most recent version. As new versions are backed up, older versions will be deleted from the Server.
- **Last Modified** - Date and time when the file was last modified
- **File Size** - Original size of the file for the given version

- To restore any version, select the appropriate row in the grid, then click the **Restore** button. File names for the older versions are automatically generated by SchoolsVault, and the downloaded file is stored in the same location as the original file.

HOW VERSIONS ARE STORED

When Versioning is enabled, you will notice some additional files on the Server. These files are stored in the same folder as the actual file.

Assume that 5 versions of **Instructions.docx** exist. You will see the following files in the repository path of the User.

File Name	File Size	Last Modified Date	Description
Instructions.docx	24.5 MB	March 30, 2010	This is the most recent version (version 5) of the file.
Instructions.docx.4_34233_1000_synver	1.5 KB	March 25, 2010	Version 4 - this is just the delta change. If the User decides to restore this version, SchoolsVault merges this delta with version 5, then sends it back to the Client.
Instructions.docx.3_3584_1000_synver	2.4 KB	March 20, 2010	Version 3
Instructions.docx.2_78484_1000_synver	2.4 KB	March 10, 2010	Version 2
Instructions.docx.1_873584_1000_synver	2.4 KB	March 09, 2010	Version 1